



Rapport analytique pour la DGRIS, Ministère des Armées

Alliance russo-chinoise dans le domaine de l'intelligence artificielle, et son évolution depuis l'invasion de l'Ukraine

Auteur : Sebastian Linke

Editeur : Vélina Tchakarova

11/09/2023

Introduction

Suite à l'invasion de l'Ukraine par la Russie, une nouvelle dynamique d'alliance entre la Russie et la Chine s'est manifestée qui pourrait bouleverser l'équilibre des pouvoirs dans la région eurasiennne et au-delà.

Pour tenter de limiter son isolement croissant sur la scène internationale après la mise en place des sanctions occidentales, la Russie se tourne dès 2014 de plus en plus vers la Chine en tant que partenaire économique, financier, technologique et militaire. De son côté, Pékin conserve une position ambiguë face à la guerre consistant à réaffirmer son autonomie stratégique et à préserver ses liens commerciaux et diplomatiques avec l'Occident, tout en profitant de l'isolement économique de la Russie et en l'utilisant comme un moyen d'accroître sa propre influence géopolitique.

Ce rapport analyse l'évolution de l'alliance russo-chinoise. Il montre pourquoi et comment cette alliance s'est constituée dans le domaine de l'intelligence artificielle, comment ces deux partenariats évoluent et ce que cette relation signifie pour l'avenir de la gouvernance mondiale. Il se concentre sur les forces géopolitiques, commerciales et géoéconomiques qui sous-tendent la relation entre Moscou et Pékin, et sur la manière dont la guerre en Ukraine a remodelé le partenariat.

Le rapport commence par définir les caractéristiques et les applications de l'IA, compare la pensée stratégique chinoise et russe dans ce domaine et explique l'écosystème des principales entreprises travaillant sur cette technologie dans les deux pays, ainsi que leurs relations avec leurs États respectifs. La deuxième partie se poursuit par une analyse de l'évolution de la coopération russo-chinoise dans le domaine de l'IA et souligne ses limites. Elle se termine par une étude de cas conjointe de l'utilisation de l'IA dans les deux pays pendant la pandémie de la COVID (pour la surveillance de masse) et par une analyse des leçons tirées par la Russie pour l'application ultérieure de l'IA à la répression de l'opposition et à la mobilisation pour la guerre (« GOULAG numérique »).

Le rapport se termine par des scénarii et des recommandations.

1. Caractéristiques et applications de l'intelligence artificielle

L'Institut des Nations unies pour la recherche sur le désarmement (UNIDIR) définit l'intelligence artificielle (IA) comme étant le « domaine d'étude consacré à rendre les machines intelligentes »¹. Toutefois, étant donné que les normes applicables aux machines considérées comme « intelligentes » évoluent constamment, il peut être plus utile d'envisager un spectre d'intelligence sur lequel les machines peuvent être placées². Tous les systèmes d'IA existants appartiennent à la catégorie générale de l'IA « étroite », ce qui signifie que leur intelligence est limitée à une seule tâche ou à un seul domaine de connaissances³. Les chercheurs estiment qu'il faudra peut-être plusieurs décennies avant de pouvoir développer une IA « générale », c'est-à-dire des systèmes capables d'une intelligence de niveau humain pour un large éventail de tâches⁴. L'approche la plus répandue pour le développement de l'IA « étroite » est l'apprentissage automatique : les machines apprenantes se voient assigner un objectif à optimiser et sont censées dériver leurs propres procédures pour atteindre cet objectif grâce à l'analyse de vastes ensembles de formation à l'aide d'algorithmes statistiques⁵. Alors que la recherche sur l'IA a débuté dans les années 1940, le domaine a connu un boom d'activité autour de 2010 en raison de trois développements convergents qui ont conduit à l'avancement de l'état de l'IA étroite : la disponibilité croissante de grands ensembles de données nécessaires pour former les algorithmes d'IA, les améliorations de l'apprentissage automatique et l'augmentation de la puissance de calcul⁶.

Lorsque l'on évoque les applications militaires de l'IA, il convient de tenir compte de trois caractéristiques essentielles de cette technologie : premièrement, l'IA peut être intégrée dans un grand nombre d'applications, deuxièmement, nombre de ces applications d'IA sont à usage dual, c'est-à-dire qu'elles ont des champs d'application à la fois civils et militaires, et troisièmement, l'intégration de l'IA dans un système peut ne pas être immédiatement reconnaissable, car il s'agit d'une capacité relativement transparente. Sayler⁷ souligne donc que l'achat de solutions d'IA ne se traduira pas par des objets définis, mais plutôt par l'intégration d'algorithmes dans une variété de systèmes plus vastes.

En conséquence, il existe une variété d'applications militaires de l'IA, notamment le renseignement, la surveillance et la reconnaissance (ISR) ; la logistique, via par exemple la maintenance prédictive ; les cyberopérations militaires ; les opérations informationnelles notamment de désinformation comme par exemple les « *deep fakes* » ; le commandement et le contrôle (C2) ; les véhicules autonomes⁸. Compte tenu du caractère dual des technologies de l'IA, Morgan et al. s'attendent à ce que la plupart des applications militaires à venir soient des adaptations de technologies développées

¹ UNIDIR, 2018, p. 2

² UNIDIR, 2018, p. 2

³ UNIDIR, 2018, p. 5

⁴ Sayler, 2020, p. 2

⁵ UNIDIR, 2018, p. 2

⁶ Sayler, 2020, p. 2

⁷ Sayler, 2020, p. 3

⁸ Sayler, 2020, p. 9-15

dans le secteur civil, y compris, mais sans s'y limiter, la reconnaissance d'images, l'analyse de textes, les voitures autonomes et les jeux⁹.

2. Réflexion stratégique chinoise sur l'intelligence artificielle

Le gouvernement chinois considère l'IA comme un composant essentiel de la puissance nationale et militaire. La priorité est donnée au plus haut niveau de l'Etat¹⁰ au développement des technologies de l'IA. Les forces armées chinoises, (Armée populaire de libération APL), prévoient que l'IA pourrait modifier fondamentalement la nature de la guerre et entraîner un passage à une guerre « intelligente », dans laquelle l'IA ferait partie intégrante des méthodes de guerre, au même titre que les technologies de l'information¹¹. Ce chapitre présente tout d'abord les stratégies et les plans nationaux de la Chine en matière de développement de l'IA. Il décrira ensuite brièvement l'écosystème chinois de l'IA. Enfin, il examinera les applications militaires actuelles et potentielles de l'IA mises en œuvre par l'APL.

2.1 Stratégies et plans nationaux

Compte tenu de la priorité accordée par la Chine à l'IA, plusieurs plans nationaux en matière de science et technologie ont mis l'accent sur son développement. Par exemple, le programme « Made in China 2025 », publié en 2015 et censé transformer la Chine en une puissance industrielle de premier plan, incluait la fabrication intelligente et la robotique, ainsi qu'un objectif de part de marché nationale pour les véhicules autonomes¹². De plus, le 13^e plan quinquennal pour l'innovation scientifique et *technologique* publié en août 2016 a donné la priorité au *big data* ainsi qu'à la fabrication intelligente et à la robotique parmi une série de nouveaux mégaprojets¹³.

Le document central qui sous-tend la stratégie chinoise en matière d'IA est toutefois le « Plan de développement de l'IA de nouvelle génération » (ci-après le Plan IA) publié en juillet 2017. Dans le cadre de ce plan, la Chine déploiera un programme tridimensionnel dans le domaine de l'IA : aborder les questions clés de la recherche et du développement (R&D), rechercher divers produits et applications et construire une industrie de l'IA d'une valeur de 141,5 milliards d'euros (150 milliards de dollars américains)¹⁴ d'ici 2030¹⁵. Par ailleurs, le plan IA formule également une stratégie nationale de fusion civilo-militaire dans le domaine de l'IA, l'une des six tâches principales définies étant de « renforcer l'intégration civilo-militaire dans le domaine de l'IA »¹⁶. À cette fin, le plan appelle à la mise en place de mécanismes pour « normaliser la communication et la coordination entre les instituts de recherche scientifique, les universités, les entreprises et les unités de l'industrie militaire » et vise à développer une nouvelle génération de technologies d'IA pour soutenir « le

⁹ Morgan et al, 2020, p. 13

¹⁰ Kania, 2017, p. 4

¹¹ Kania, 2017, p. 4, 12

¹² Kania, 2017, p. 9

¹³ Kania, 2017, p. 9

¹⁴ La conversion du dollar américain en euro est effectuée tout au long de ce document en utilisant un taux de change de 1 € = 1,06 \$ US (taux de change au 26 février 2023).

¹⁵ Kania, 2017, p. 9

¹⁶ Conseil d'État, 2017, p. 21

commandement et la prise de décision, la déduction militaire, l'équipement de défense et d'autres applications »¹⁷.

Selon Bernhard Seyringer, le développement de l'IA en Chine, conformément au « plan de développement artificiel de nouvelle génération », est divisé en trois phases. La phase initiale, achevée en 2020, a vu la Chine égaler les prouesses d'autres pays avancés dans le domaine de l'IA. D'ici à 2025, la Chine entend accroître sa compétitivité dans divers secteurs de l'IA et établir de nouvelles normes technologiques en réalisant des avancées significatives dans la recherche fondamentale. Cela pourrait propulser la Chine au premier rang mondial des applications de l'IA. Enfin, d'ici 2030, la Chine aspire à devenir le premier centre mondial d'innovation en matière d'IA¹⁸.

Tandis que la Chine a officiellement déclaré dans le « plan de développement artificiel de nouvelle génération » son ambition d'être le leader mondial de l'intelligence artificielle au cours de la prochaine décennie, il est essentiel de reconnaître que Pékin est l'égal des États-Unis dans les applications commerciales et de sécurité nationale de l'IA et montre la tendance de les dépasser¹⁹. Les bouleversements technologiques à venir, en grande partie dus à l'IA, sont sur le point de remodeler les réseaux économiques et sécuritaires mondiaux, à l'instar de l'influence des semi-conducteurs, des ordinateurs et de l'internet²⁰. En plus d'être la pierre angulaire de la transformation numérique, l'IA devrait doter Pékin d'outils puissants pour consolider sa gouvernance, en augmentant sa capacité de surveillance, de collecte et d'interprétation des données, affectant à la fois les populations et les gouvernements à la fois en Chine et à l'étranger.

La Chine tire parti de son accès à de vastes ensembles de données pour accélérer le développement d'algorithmes d'apprentissage automatique, à un rythme inégalé par les sociétés démocratiques en raison de leurs préoccupations en matière de stockage, de collecte et de sécurité des données. En outre, la Chine amplifie ses prouesses nationales, tant scientifiques que militaires en matière d'IA en fondant des centres d'excellence, en promouvant des programmes universitaires et de sécurité, et en lançant des programmes financés par l'État pour des équipes nationales, locales et universitaires (Seyringer, 2021). Outre ses avancées dans le domaine de l'IA, la Chine progresse également dans des domaines tels que la reconnaissance faciale, la « *fintech* », les drones armés et les réseaux 5G, où elle domine le développement technologique. Il est intéressant de noter que dans certains domaines tels que la *fintech*, la technologie vocale ou la reconnaissance faciale, la Chine a obtenu de meilleurs résultats que les États-Unis, principalement en raison des contraintes éthiques, morales, constitutionnelles ou normatives auxquelles ces derniers et d'autres systèmes politiques démocratiques sont confrontés (Allison & Schmidt, 2020).

¹⁷ Conseil d'État, 2017, p. 21

¹⁸ Seyringer B. (2021, 10 juin) ; Artificial Intelligence : Une masse d'assassin chinois ; L'horizon de la défense.

<https://www.thedefencehorizon.org/post/artificial-intelligence-a-chinese-assassin-s-mace>

¹⁹ Allison G., Schmidt E. (2020) Is China Beating the U.S. to AI Supremacy ; Belfer Center for Science and International Affairs.

<https://www.belfercenter.org/publication/china-beating-us-ai-supremacy>

²⁰ Ibid.

Des ouvrages tels que « *AI Superpowers : China, Silicon Valley, and the New World Order* » de Kai-Fu Lee (président-directeur général de Sinovation Ventures) et « *AI and the Future of Power* » de Rajiv Malhotra fournissent un compte rendu perspicace des progrès et des objectifs de la Chine en matière d'IA. Le dynamisme, l'ampleur et la résolution des efforts déployés par la Chine pour atteindre la suprématie en matière d'IA nécessitent un examen approfondi. L'augmentation des investissements, le nombre croissant de scientifiques et de brevets dans le domaine des technologies de l'IA, ainsi que l'essor du financement par le secteur privé témoignent de l'engagement de la Chine. De la *fintech* à la reconnaissance faciale en passant par les plateformes commerciales et l'internet des objets, la Chine ouvre la voie dans de multiples domaines. En outre, les drones alimentés par l'IA et les réseaux 5G donnent à la Chine un avantage sur le plan mondial en raison de la demande croissante des gouvernements en Moyen-Orient et en Afrique.

Les technologies numériques, telles que l'IA et la science des données, sont appelées à susciter des innovations technologiques dans divers domaines tels que la santé publique et les questions climatiques. Toutefois, leur application à grande échelle soulève de nombreux dilemmes éthiques, juridiques et sociétaux²¹, que les États-Unis et la Chine abordent différemment.

Dans le cadre des travaux visant à contrer les « tempêtes dangereuses » auxquelles le pays est confronté Pékin a appelé à une surveillance accrue de l'IA. Le gouvernement chinois a, lors d'une réunion de la Commission de la sécurité nationale, convenu qu'il était nécessaire d'améliorer la gestion de la sécurité des données des réseaux et de l'IA.

En 2023, Pékin a initié une vaste campagne d'éradication des menaces à la sécurité nationale en restreignant l'accès aux données, en menant des perquisitions dans des sociétés de conseil étrangères et en renforçant les lois contre l'espionnage. Elle a également pris des mesures pour renforcer son contrôle sur l'IA. Un projet de loi récemment dévoilé exige que tous produits d'IA soit soumis à un contrôle des normes de sécurité avant d'être mis sur le marché. Le texte stipule que les produits d'IA devront refléter les « valeurs socialistes fondamentales » et ne devront pas « comporter de contenu visant à subvertir le pouvoir de l'État ». Pékin considère également que les « *deep fakes* » (images et sons générés par l'IA qui peuvent être d'un réalisme stupéfiant) constituent un « danger pour la sécurité nationale et la stabilité sociale ».

La transformation numérique pourrait engendrer des sociétés de surveillance, où l'État contrôlerait toutes les collectes et toutes les analyses des données. Dans ce contexte, la Chine pourrait créer un précédent pour les futurs régimes autoritaires du Moyen-Orient, d'Afrique et d'Asie. Andrew Michta affirme que « *nous devons reconnaître que nous ne sommes pas confrontés à la « Chine » en tant que civilisation, mais plutôt à une puissance communiste dont l'idéologie a toujours été fondamentalement totalitaire. Ce qui se déroule sous nos yeux - et qui est en cours depuis trois décennies, depuis la fin de la guerre froide - est la deuxième étape, peut-être décisive et finale, du*

²¹ Coeckelbergh C. (2020, 19 mai) Corona-App : Ethische, rechtliche und gesellschaftliche Fragen ; Der Standard.

<https://www.derstandard.at/story/2000117457544/corona-app-ethische-rechtliche-und-gesellschaftliche-fragen>

conflit entre la démocratie libérale et le communisme »²², ou plutôt entre la démocratie et la dictature.

2.2 L'écosystème chinois de l'IA

Le gouvernement chinois, et donc par extension le Parti communiste chinois (PCC), joue un rôle essentiel dans le développement de l'écosystème de l'IA du pays. Entre 2005 et 2015, il a augmenté ses dépenses en matière d'IA de 350% et l'on estime aujourd'hui qu'il est très proche des niveaux de dépenses des États-Unis. Toutes les activités, y compris le développement technologique, sont contrôlées au plus haut niveau par le Comité central du PCC. En outre, la Commission militaire centrale (CMC) joue un rôle clé dans l'élaboration des politiques et la coordination des efforts concernant les applications civiles et militaires de l'IA²³. En outre, le "National Science and Technology Leading Group", un organe délibératif et consultatif du Conseil d'État qui a été dissous en 2023, jouait un rôle important dans l'élaboration des politiques et les efforts de coordination en matière de science et de technologie.²⁴

Les efforts de recherche en matière d'IA et d'automatisation pertinents pour l'armée s'étendent aux institutions universitaires, aux laboratoires nationaux, aux instituts de recherche de l'industrie de la défense et aux instituts de recherche de l'Armée populaire de libération (APL). L'Académie chinoise des sciences (CAS) joue un rôle clé, car de nombreux instituts associés à cette institution sont impliqués dans la recherche sur l'IA. Il s'agit notamment de l'Institut des machines intelligentes, de l'Institut d'automatisation et du Laboratoire clé national pour la reconnaissance des formes. En outre, le Laboratoire clé de traitement intelligent de l'information de l'Institut de technologie informatique poursuit des recherches sur le traitement et la traduction du langage naturel et sur les interfaces homme-machine intelligentes. En outre, le CAS participe à divers efforts de recherche conjoints dans le domaine de l'IA, en partenariat avec d'autres universités et des entreprises privées. Outre la CAS, d'importantes institutions universitaires impliquées dans la recherche militaire comprennent l'université Tsinghua, qui a créé en 2017 son "Military-Civil Fusion National Defense Peak Technologies Laboratory" (laboratoire des technologies de pointe de la défense nationale) afin de poursuivre les doubles avancées en matière d'IA, ainsi que l'université Beihang, qui est étroitement liée au développement de technologies aéronautiques et astronautiques militaires, y compris les véhicules sous-marins autonomes sans pilote et les drones intelligents, notamment pour l'essaimage et l'association homme-machine sans pilote.²⁵

En 2017, le Ministère de la science et de la technologie chinois a désigné les entreprises technologiques Baidu, Alibaba, Tencent et iFlytek comme membres d'une « équipe nationale de

²² Michta A.A. (2020, 7 mai) The Building Blocks of a China Strategy. The American Interest. <https://www.the-american-interest.com/2020/05/07/the-building-blocks-of-a-china-strategy/>

²³ Hynek & Solovyeva, 2022, p. 65

²⁴ Hynek & Solovyeva, 2022, p. 65; Wei, C., Hu, T. & Liao, Z. (2023, 7 March). A Guide to China's 2023 State Council Restructuring. <https://npcobserver.com/2023/03/china-npc-2023-state-council-reorganization/>

²⁵ Kania, 2017, p. 47-49

l'IA »²⁶. Ces entreprises reçoivent un soutien des gouvernements national et locaux, en échange de quoi elles doivent construire des « plateformes d'innovation ouverte » dans des domaines technologiques spécifiques, auxquelles d'autres entreprises peuvent participer²⁷. En 2019, l'« équipe nationale d'IA » chinoise a été élargie à 15 entreprises, dont Huawei pour les logiciels et le matériel (voir la figure 1 ci-dessous)²⁸. Parallèlement, la Chine possède un écosystème de *start-ups* dynamique²⁹. Les *start-ups* chinoises spécialisées dans l'IA ont remporté plusieurs concours internationaux d'IA, ce qui montre qu'elles sont à la pointe de la R&D, notamment en matière de reconnaissance vocale et de vision par ordinateur³⁰.

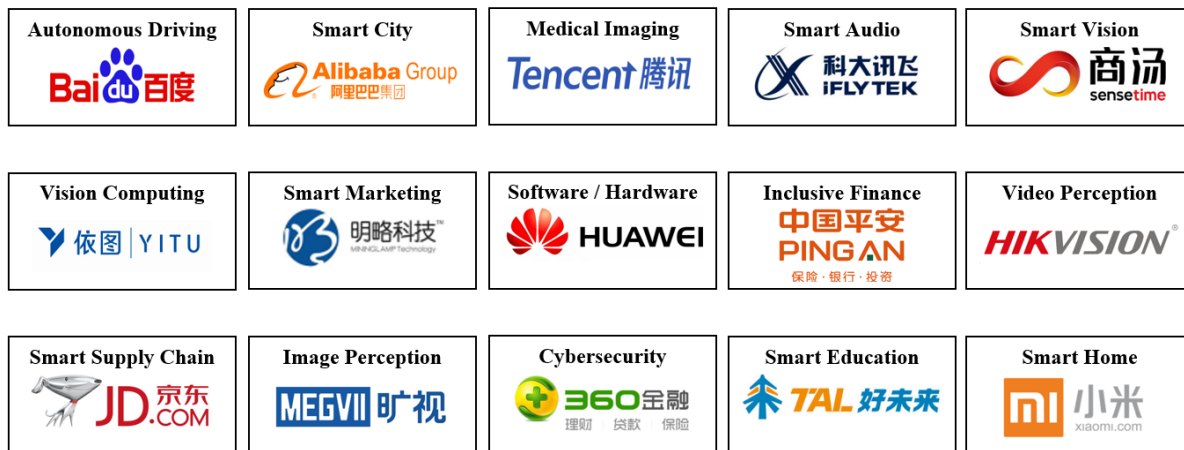


Figure 1: Membres de « l'équipe nationale d'IA » de la Chine, Source : Larsen, 2019, p. 17

Comme cela a déjà été mentionné, l'APL souhaite tirer parti des progrès du secteur civil dans le développement de l'IA par le biais d'une stratégie nationale de fusion civile-militaire, tout en poursuivant elle-même un programme de R&D étendu³¹. Cette stratégie sera dirigée par la Commission du Comité central pour le développement de l'intégration civilo-militaire, qui a été créée en 2017 sous la direction de Xi Jinping lui-même³². Au sein de l'APL, la Commission des sciences et des technologies de la CMC et son nouveau Comité d'orientation de la recherche scientifique militaire (*Military Science Research Steering Committee*) seront responsables du programme de R&D de l'APL et de la fusion civile-militaire³³. L'APL a également créé des mécanismes à des niveaux inférieurs pour mettre en œuvre l'intégration civile-militaire, notamment la création de l'Institut de recherche sur les équipements intelligents pour l'intégration civile-militaire, qui se concentre en particulier sur la robotique, les systèmes sans pilote et l'intelligence artificielle³⁴. Soulignant l'importance stratégique attribuée à ce programme, la Commission de la science et de la technologie de la CMC et le Ministère de la science et de la technologie ont

²⁶ Larsen, 2019, p. 16

²⁷ Larsen, 2019, p. 16

²⁸ Larsen, 2019, p. 16-17

²⁹ Kania, 2017, p. 6

³⁰ Kania, 2017, p. 6

³¹ Kania, 2017, p. 12

³² Kania, 2017, p. 19

³³ Kania, 2017, p. 19

³⁴ Hynek & Solovyeva, 2022, p. 65

également publié conjointement le 13th *Five-Year Science and Technology Military-Civil Fusion Plan* (Plan quinquennal de fusion civile-militaire de la science et de la technologie) en 2017³⁵.

L'APL a commencé aussi à mettre en place des partenariats avec le secteur privé en vue d'une fusion militaire-civile dans le domaine de l'IA. Ainsi, iFlytek, une *start-up* spécialisée dans la reconnaissance vocale intelligente et les produits de conversion de la parole en texte, travaillerait avec l'APL sur un module de reconnaissance et de synthèse vocales. HikVision, une *start-up* détenue par l'entreprise publique *China Electronics Technology Group Corporation* (CETC), a collaboré avec l'APL pour utiliser sa technologie de surveillance vidéo basée sur l'IA à des fins de défense et de sécurité nationales³⁶. En outre, plusieurs nouveaux instituts de recherche et laboratoires conjoints ont été créés pour travailler sur les avancées à double usage de la technologie de l'IA³⁷. Par exemple, un laboratoire commun pour les technologies de commandement et de contrôle intelligentes a été créé par CTEC et Baidu³⁸.

2.3 Applications militaires de l'intelligence artificielle

Comme mentionné plus haut, l'APL prévoit que l'IA puisse transformer fondamentalement le caractère de la guerre. En conséquence, elle exploite l'IA pour des applications militaires comme les systèmes autonomes sans pilote, la fusion de données, le traitement de l'information et l'analyse du renseignement, les jeux de guerre, la simulation et l'entraînement, la défense, l'offensive et le commandement dans les systèmes d'information (cyberguerre), ainsi que le soutien intelligent à la prise de décision par le commandement. Sur la base de l'analyse de 58 articles de journaux rédigés entre 2016 et 2020 par des officiers de l'APL, des ingénieurs de l'industrie de la défense et des universitaires des principales universités chinoises travaillant sur l'IA et les futurs systèmes d'armes, M. Fediasuk constate que les experts chinois prévoient que l'IA améliorera la détection, le ciblage et les frappes contre les cibles militaires³⁹. Il note que les experts chinois considèrent que l'IA peut réduire les coûts de signalisation ou de déploiement des forces, en particulier grâce à l'utilisation de munitions intelligentes, de véhicules aériens sans pilote et de logiciels ISR⁴⁰. Si la réflexion initiale de l'APL sur l'IA a été façonnée par l'analyse des initiatives militaires américaines, Elsa Kania estime que l'APL pourrait à l'avenir suivre une voie différente, compte tenu de sa culture stratégique et de sa dynamique organisationnelle propres.⁴¹ Elsa Kania souligne notamment que l'APL se concentre depuis les années 1990 sur le développement d'armes « cartes maîtresses » qui ciblent les vulnérabilités des réseaux de combat américains⁴².

Dans un rapport publié en 2017, Elsa Kania affirme que l'APL semble être « très axée sur l'utilisation de l'IA dans la simulation, le jeu de guerre et l'entraînement, ainsi que pour soutenir la

³⁵ Kania, 2017, p. 19

³⁶ Kania, 2017, p. 20

³⁷ Kania, 2017, p. 20

³⁸ Hynek & Solovyeva, 2022, p. 65

³⁹ Fediasuk, 2020, 2

⁴⁰ Fediasuk, 2020, p. 2

⁴¹ Kania, 2017, p. 4-5

⁴² Kania, 2017, p. 4-5

connaissance de la situation et la prise de décision du commandement ».⁴³ L'intérêt de l'APL pour l'utilisation de l'IA dans la simulation et l'entraînement est lié à son manque d'expérience au combat, ce qui signifie que les simulations et les jeux de guerre informatisés jouent déjà un rôle clé dans son entraînement ; l'APL pourrait donc tirer parti de l'IA pour améliorer le réalisme de ces exercices⁴⁴. En ce qui concerne l'utilisation de l'IA pour améliorer la connaissance de la situation et faciliter la prise de décision opérationnelle par le commandement, l'APL travaille sur divers systèmes basés sur l'IA pour fusionner de manière autonome des informations provenant de multiples sources de renseignement en une seule image opérationnelle commune⁴⁵. L'APL a commandé divers projets qui exploitent l'apprentissage profond afin d'améliorer la reconnaissance d'images et la différenciation d'images photographiques, infrarouges, radar et d'autres images de capteurs⁴⁶. Dans le même temps, l'APL a donné la priorité à « l'intelligentisation » de ses systèmes d'information de commandement au plus haut niveau et vise à développer une assistance intelligente à la prise de décision opérationnelle⁴⁷. Selon Morgan *et al*, l'APL espère que ces systèmes agiront à l'avenir comme un « officier d'état-major numérique » qui fournira des informations, des recommandations et des suggestions de planification⁴⁸.

Dans le même temps, l'APL développe des robots autonomes⁴⁹, dont certains sont dotés au moins d'un degré limité d'autonomie⁵⁰. La Chine a notamment beaucoup investi dans le développement d'essaims de drones aériens (UAV) et de drones de surface navals (USV)⁵¹. Par exemple, le drone hélicoptère Blowfish A2 utilise la vision par ordinateur pour reconnaître les cibles et pour effectuer des missions de combat complexes de manière autonome, tout en étant capable de former un essaim⁵². La Chine a fait des progrès en matière de technologie d'essaim à plusieurs reprises : en juin 2017, l'entreprise publique CETC a testé un essaim de 119 drones à voilure fixe qui ont effectué des décollages assistés par catapulte et ont montré des formations complexes⁵³. En décembre 2017, la Chine a établi des records mondiaux en testant un essaim de 1180 quadcoptères lors d'un salon aéronautique à Guangzhou⁵⁴. Bien que l'APL semble avoir moins investi dans le développement de véhicules terrestres sans pilote (UGV) que dans celui de drones aériens, elle a tout de même mis au point des systèmes innovants tels que le *Sharp Claw I*, un UGV à six roues, et le *Sharp Claw II*, un UGV armé plus petit et porté par le premier⁵⁵. En outre, l'APL a également développé des systèmes

⁴³ Kania, 2017, p. 21

⁴⁴ Kania, 2017, p. 36

⁴⁵ Kania, 2017, 29 ; Morgan et al. 2020, p. 66 ; Morgan et al. 2020, p. 82

⁴⁶ Morgan et al, 2020, p. 66

⁴⁷ Kania, 2017, p. 29

⁴⁸ Morgan et al, 2020, p. 82

⁴⁹ Morgan et al, 2020, p. 62

⁵⁰ Kania, 2019, p. 31-32 ; Kania, 2021, 535

⁵¹ Morgan et al, 2020, p. 61

⁵² Hynek & Solovyeva, 2022, p. 56

⁵³ Kania, 2017, p. 23

⁵⁴ Morgan et al, 2020, p. 62

⁵⁵ Morgan et al, 2020, p. 63-64

robotiques maritimes et aurait déjà déployé le *Jinghai USV*, un petit patrouilleur sans pilote capable de naviguer de manière autonome et d'éviter les obstacles⁵⁶.

3. Réflexion stratégique russe sur l'intelligence artificielle

À l'instar de Pékin, Moscou considère l'IA comme une technologie clé pour ses futures capacités militaires. Dans un discours prononcé en 2017, Vladimir Poutine a publiquement souligné l'importance de l'IA en déclarant : « L'intelligence artificielle est l'avenir, non seulement pour la Russie, mais pour toute l'humanité. Elle s'accompagne d'opportunités colossales, mais aussi de menaces difficilement prévisibles. Celui qui deviendra le *leader* dans ce domaine deviendra le maître du monde »⁵⁷. Ces dernières années, le Ministère russe de la défense a constamment investi dans la Recherche et le Développement en matière d'IA. La société allemande de services logiciels SAP a estimé que l'État russe a entre 2007 et 2017 dépensé 343 millions d'euros (363,5 millions de dollars américains) pour des projets scientifiques dans le domaine de l'IA, ce qui correspond à un investissement annuel de 34 millions d'euros (36 millions de dollars américains). Toutefois, ce chiffre est bien inférieur à celui des États-Unis, qui dépensent des milliards par an pour la recherche sur l'IA⁵⁸. La structure de ce chapitre reflète celle du chapitre précédent : il présente tout d'abord les stratégies et les plans nationaux de la Russie en matière de développement de l'IA. Suit une description de l'écosystème russe de l'IA. Enfin, sont abordées les applications militaires actuelles et potentielles de l'IA visées par l'armée russe.

3.1 Stratégies et plans nationaux

En mars 2018, le gouvernement russe a publié sa première proposition officielle sur l'IA. Ce document fait 10 recommandations pour faire progresser l'IA en Russie⁵⁹. Dans le cadre de son programme « Économie numérique », publié en décembre 2018, le gouvernement russe a chargé Sberbank, une banque publique qui a depuis 2011 une branche technologique Sberbank Technology, de rédiger une feuille de route sur le développement de l'IA et des neurotechnologies. Cette feuille de route publiée en octobre 2019 décrit les sous-technologies d'IA pertinentes, telles que le traitement du langage naturel, la reconnaissance vocale et la vision par ordinateur⁶⁰. Elle estime qu'un montant total d'environ 5,4 milliards d'euros (392 milliards de roubles)⁶¹ sera nécessaire pour le développement de l'IA jusqu'en 2024⁶². Avant même la publication de cette feuille de route, Vladimir Poutine avait chargé le gouvernement d'élaborer une stratégie nationale en matière d'IA. Cette dernière également rédigée par Sberbank, a été approuvée en octobre 2019 et doit servir de base à la planification et à la mise en œuvre des programmes étatiques liés à l'IA jusqu'en 2030⁶³.

⁵⁶ Morgan et al, 2020, p. 64-65

⁵⁷ "'Celui qui est à la tête de l'IA dirigera le monde' : Poutine aux enfants russes à l'occasion de la journée du savoir", 2017

⁵⁸ Morgan et al, 2020, p. 91

⁵⁹ Hynek & Solovyeva, 2022, p. 62

⁶⁰ Edmonds et al, 2021, p. 20

⁶¹ Conversion des roubles en euros en utilisant le taux de change annuel en 2019 de 1 € = 72,45

⁶² Edmonds et al, 2021, p. 20

⁶³ Edmonds et al, 2021, p. 21

Pour atteindre les objectifs définis dans la stratégie nationale, les dirigeants russes ont également ordonné l'élaboration d'un projet fédéral d'IA en tant que facette supplémentaire du programme « Économie numérique »⁶⁴. Encore une fois rédigé par Sberbank, le document approuvé par le gouvernement en août 2020, a non seulement ajouté des indicateurs de financement et de performance aux objectifs définis dans la stratégie nationale mais a aussi permis de définir un échéancier pour l'élaboration et la mise en œuvre des programmes d'IA⁶⁵. Toutefois, il est à noter qu'il n'existe pas encore de stratégie proprement militaire en matière d'IA en Russie⁶⁶.

3.2 L'écosystème russe de l'IA

L'écosystème russe de l'IA est constitué de groupes d'activités interconnectées entre le gouvernement, les entreprises d'État, l'armée, les universités et le secteur privé. Les principales caractéristiques de cet écosystème sont qu'il est dirigé par des entreprises publiques et qu'un montant disproportionné du financement du secteur de l'IA provient du gouvernement. En 2018, 67% du financement de la R&D en IA en Russie provenait du budget fédéral, alors qu'aux États-Unis 77% du financement de la R&D était assuré par le secteur privé⁶⁷. Quant à la Chine, il est difficile de faire la distinction entre les financements qui proviennent du milieu public et ceux délivrés par le secteur privé. De plus, le gouvernement russe a créé des incubateurs (par exemple, le Skolkovo), des fonds (par exemple, le Fonds russe d'investissement direct) et des initiatives (par exemple, l'Initiative technologique nationale) visant à faciliter le développement des technologies de l'IA. La fondation Skolkovo, en particulier, joue un rôle central dans l'écosystème russe de l'IA, car la plupart des activités de R&D dans le domaine de l'IA passent par elle. Devenu un site institutionnel de financement et d'accueil des jeunes prodiges, le parc technologique (Skolkovo) apporte également son soutien à l'intégration de ces élèves sur des marchés internationaux plus vastes. Outre Skolkovo, d'importants centres de recherche sur l'IA existent dans des regroupements autour des universités d'État, notamment l'Institut de physique et de technologie de Moscou, l'École supérieure d'économie et l'Université fédérale d'Extrême-Orient⁶⁸.

La Sberbank mentionnée plus haut joue un rôle central dans l'écosystème russe de l'IA, puisque le gouvernement lui a confié l'élaboration de tous les principaux documents nationaux relatifs à l'IA. Si ça paraît surprenant que le gouvernement russe ait chargé une banque de rédiger de tels documents, German Gref, PDG et président du conseil d'administration de la Sberbank, a adopté une stratégie visant à transformer la banque en une institution financière de haute technologie depuis qu'il a pris ses fonctions en 2007⁶⁹. Avec sa « Stratégie 2020 » présentée en 2017, Sberbank a lancé sa transformation en une entreprise technologique universelle avec son propre écosystème de services financiers et non financiers⁷⁰. Parallèlement, le rôle de premier plan joué par Sberbank dans le développement de l'IA en Russie reflète les liens étroits entre l'entreprise et le gouvernement russe

⁶⁴ Edmonds et al, 2021, p. 21

⁶⁵ Edmonds et al, 2021, p. 21-22

⁶⁶ Hynek & Solovyeva, 2022, p. 61

⁶⁷ Nocetti, 2020, p. 21

⁶⁸ Edmonds et al, 2021, p. 34, 63-64

⁶⁹ Sberbank, n.d.

⁷⁰ Sberbank, n.d. ; Sberbank, 2020

: le Ministère des finances détient la majorité des actions de Sberbank, soit 50 % plus une action de la société qu'il a acquise auprès de la Banque de Russie en utilisant des fonds du Fonds national de la richesse en avril 2020⁷¹. En outre, il existe des liens personnels entre Sberbank et le Kremlin. German Gref est un allié de longue date de Vladimir Poutine⁷². M. Poutine et M. Gref ont tous deux travaillé dans l'administration locale de Saint-Petersbourg dans les années 1990⁷³. Pendant le premier et le deuxième mandat présidentiel de Vladimir Poutine, M. Gref a été ministre du développement économique et du commerce entre 2000 et 2007⁷⁴.

Sberbank	
Structure de l'entreprise et actionnaires	• Ministère russe des finances : 50 % + 1 action • Investisseurs nationaux et internationaux : 50% - 1 action
Les dirigeants	• Président du conseil de surveillance : Anton Siluanov (ministre russe des finances) • Directeur général et président du conseil d'administration : German Gref

D'autres grandes entreprises publiques, telles que Rostec, le plus important conglomérat russe dans le domaine de la Défense, ou les entreprises énergétiques Gazprom Neft et Lukoil, travaillent sur un certain nombre de technologies d'IA. Néanmoins, contrairement à Sberbank, elles ne jouent pas un rôle significatif dans l'élaboration de la stratégie officielle de l'État en la matière. Par ailleurs, les entreprises technologiques privées ne représentent qu'une part mineure des efforts consentis par le gouvernement pour développer l'IA. Yandex, la plus grande entreprise technologique de Russie, a développé quelques produits liés à l'IA, mais n'a joué qu'un rôle secondaire dans le développement de l'écosystème russe de l'IA dans son ensemble. Yandex a toutefois formé l'« AI Russia Alliance » avec d'autres grandes entreprises telles que Sberbank, Mail.ru, Gazprom Neft, MTS et le Fonds d'investissement direct russe, qui a réussi à fournir un retour d'information important sur les initiatives étatiques⁷⁵.

Le Ministère russe de la Défense joue également un rôle clé dans l'écosystème de l'IA en tant que moteur de l'innovation. A l'instar du modèle adopté par les États-Unis, dans celui adopté par la Russie, l'État joue le rôle de bailleur de fonds pour les projets civils innovants ayant des applications militaires⁷⁶. Les domaines technologiques prioritaires sont la reconnaissance faciale et vocale, l'imagerie et le cerveau⁷⁷. Au sein du même ministère, le Département principal de la recherche et du soutien technologique des technologies avancées et la Fondation pour la recherche avancée sont

⁷¹ "Government acquires Sberbank shares from Central Bank for \$29bln", 2020

⁷² Edmonds et al, 2021, p. 25

⁷³ Munzinger-Archiv, 2022

⁷⁴ Munzinger-Archiv, 2022

⁷⁵ Edmonds et al, 2021, p. 63-67

⁷⁶ Nocetti, 2020, p. 24

⁷⁷ Nocetti, 2020, p. 24

chargés de mener ces initiatives⁷⁸. Depuis 2015, la Fondation, qui dispose d'un budget annuel d'environ 60 millions d'euros et regroupe 46 laboratoires, a concentré ses efforts en particulier sur la robotique militaire⁷⁹. Néanmoins, l'intégration directe militaro-civile, telle que poursuivie par la Chine, est relativement faible à l'heure actuelle⁸⁰. Parmi les autres organisations responsables des aspects militaires liés au développement et à l'application de l'IA figurent la Commission du Ministère de la Défense pour le développement de systèmes robotiques à des fins militaires, dirigée par le Ministre russe de la Défense, Sergei Choïgou, et le Centre principal de recherche et d'essai en robotique du Ministère de la Défense⁸¹. L'innovation militaire est facilitée par Rostec et d'autres entreprises de Défense⁸². Enfin, la technopole ERA, inaugurée en juin 2018, sera la clé de voûte de tous les développements en matière d'IA et d'autres domaines stratégiques tels que la cybersécurité et les nanotechnologies. Sur son campus de Krasnodar, elle regroupe près de 12 entreprises et 600 chercheurs dont elle prévoit d'augmenter le nombre (pour atteindre les 2000 individus)⁸³.

3.3 Applications militaires de l'intelligence artificielle

La Russie poursuit des activités de R&D en matière d'IA pour plusieurs applications militaires. Cependant, Edmonds et al. notent que l'armée russe accorde des fonds importants au développement de drones aériens, terrestres et maritimes et de leurs composants⁸⁴. Au cours de sa campagne militaire en Syrie, l'armée russe a déjà testé les véhicules, e.g. Uran-6 et Uran-9 UGV⁸⁵. Elle a également effectué plus de 23 000 missions de vol avec des drones, principalement des drones ISR à courte et moyenne portée⁸⁶. Bien que la plupart des unités testées soient encore télécommandées, leur niveau d'autonomie pourrait croître à mesure que les logiciels s'améliorent⁸⁷.

Le Comité militaro-industriel russe s'est fixé pour objectif de robotiser 30% de ses équipements militaires d'ici à 2025⁸⁸. Morgan et al. considèrent qu'il s'agit d'un objectif très ambitieux compte tenu des divers obstacles auxquels la Russie a été confrontée lors du développement des drones aériens⁸⁹. A titre d'exemple, les mêmes auteurs considèrent que la Russie n'est pas encore en mesure de mettre sur le marché un drone de combat aérien susceptible de voler à moyenne altitude et doté d'une longue autonomie⁹⁰. Julien Nocetti note que la Russie n'a jusqu'à présent développé que des prototypes de robots militaires « intelligents » possédant des systèmes de contrôle utilisant l'intelligence artificielle⁹¹. Pourtant, plusieurs entités industrielles de défense russes ont ces

⁷⁸ Nocetti, 2020, p. 24

⁷⁹ Nocetti, 2020, p. 24

⁸⁰ Edmonds et al, 2021, p. 38

⁸¹ Hynek & Solovyeva, 2022, p. 66

⁸² Edmonds et al, 2021, p. 38 ; Hynek & Solovyeva, 2022, p. 66

⁸³ Nocetti, 2020, p. 25

⁸⁴ Edmonds et al, 2021, p. 77 ; Morgan et al, 2020, p. 84

⁸⁵ Edmonds et al, 2021, p. 115-116

⁸⁶ Edmonds et al, 2021, p. 115

⁸⁷ Morgan et al, 2020, p. 84

⁸⁸ Morgan et al, 2020, p. 85

⁸⁹ Morgan et al, 2020, p. 85

⁹⁰ Morgan et al, 2020, p. 85

⁹¹ Nocetti, 2020, p. 24-25

dernières années testé des drones de combat dotés d'IA. Tel a été le cas en septembre 2019, avec le drone de combat S-70 Okhotnik ⁹².

Par ailleurs, la Russie semble également particulièrement intéressée par la formation d'essaims, notamment dans le domaine maritime⁹³. Selon Morgan et al, cette dernière a néanmoins un temps de retard dans le secteur en comparaison à ses homologues américain et chinois⁹⁴.

En 2018, Vladimir Poutine a également mis en avant de nouvelles armes nucléaires semi-autonomes voire complètement autonomes supposées compléter l'arsenal russe⁹⁵. Parmi ces armes, seul le missile hypersonique Avangard est déjà en service⁹⁶. Cependant, en janvier 2023, l'agence TASS a rapporté que la Russie avait également commencé la production de la première série de torpilles furtives pilotables à distance de type Poséidon. Ce type de torpille a la particularité de pouvoir fonctionner de manière autonome et d'être alimentée par un petit réacteur nucléaire lui permettant de parcourir de longues distances⁹⁷.

La Russie a également une longue tradition de développement de systèmes défensifs plus ou moins autonomes. En 1979, l'Union soviétique construisait ainsi le premier système de protection active pour les véhicules blindés. Son système de protection active le plus récent, baptisé Afghant, est capable de détecter et de suivre simultanément jusqu'à 40 cibles terrestres et 25 cibles aériennes et aurait déjà été ajouté aux chars T-14 Armata. Le système de défense antiaérien S-400 Triumf est quant à lui capable de détecter et de cibler de manière autonome jusqu'à 36 menaces aériennes à une distance de 250 kilomètres. En 2018, la Russie a également commencé à tester un nouveau système de contrôle automatisé qui devrait équiper l'ensemble des systèmes de défense antiaérienne (S-300, S-400 et Pantsir-S) ⁹⁸.

En outre, la Russie a commencé à intégrer des éléments d'IA dans son infrastructure de commandement et de contrôle, en particulier dans ses plates-formes de planification et d'aide à la décision. Près de la moitié des financements publics russes dans le domaine de l'IA ont été consacrés à des projets d'analyse de données (33%) et à des systèmes d'aide à la décision (16,5%)⁹⁹. Le Centre national de gestion de la défense de la Russie, chargé de l'évaluation continue et de la coordination de toutes les activités militaires et de sécurité nationales et internationales, utiliserait déjà l'IA pour collecter et organiser l'information.¹⁰⁰ L'armée russe a également l'intention d'exploiter l'IA au niveau opérationnel en se concentrant sur l'intégration d'informations provenant de différentes plates-formes dans les branches militaires afin d'améliorer la coordination des forces et la rapidité de la prise de décision¹⁰¹. Au niveau tactique, la Russie poursuit par exemple des initiatives visant

⁹² Edmonds et al, 2021, p. 118

⁹³ Edmonds et al, 2021, p. 111-113

⁹⁴ Morgan et al, 2020, p. 85

⁹⁵ Edmonds et al, 2021, p. 89

⁹⁶ Edmonds et al, 2021, p. 91

⁹⁷ Faulconbridge, 2023

⁹⁸ Morgan et al, 2020, p. 86

⁹⁹ Morgan et al, 2020, p. 87-88

¹⁰⁰ Edmonds et al, 2021, p. 95, 144-146

¹⁰¹ Edmonds et al, 2021, p. 96-97

à développer des systèmes d'information et de contrôle à base d'IA à bord de ses avions de chasse, systèmes qui pourraient aider le pilote à gérer le flux d'informations¹⁰².

La Russie peut également utiliser l'IA dans ses activités hybrides (en « zone grise »), e.g. la cyberguerre, la guerre électronique, les opérations d'influence, les campagnes de propagande et la désinformation. Elle y a ainsi eu recours pour produire des « *deep fakes* ». Elle a également mis au point un système de guerre électronique automatisé, le RB109-A Bylina, capable d'analyser de manière totalement autonome des situations de combat, d'identifier des cibles, de décider comment les désactiver et, enfin, d'envoyer des ordres aux unités de guerre électronique sur le terrain¹⁰³.

4. Évolution de la coopération entre la Russie et la Chine dans le domaine de l'intelligence artificielle

Bien que le gouvernement russe ait souvent manifesté un intérêt particulier pour collaborer avec d'autres pays dans le domaine de l'IA, Edmonds et al. notent que les partenariats avec des entreprises étrangères n'ont joué qu'un rôle limité dans le développement de l'IA en Russie. Outre les sanctions imposées depuis 2014 par les États-Unis et l'Union européenne, l'engagement limité des entreprises technologiques asiatiques sur le marché russe peut s'expliquer par la taille relativement modeste de ce dernier et au manque d'incitations pour les entrepreneurs à opérer dans le pays¹⁰⁴.

L'entreprise technologique chinoise Huawei et l'entreprise sud-coréenne Samsung, toutes deux présentes en Russie, font exception à la règle. Ces dernières années, la Chine est devenue le principal partenaire de la Russie dans le domaine des hautes technologies en général et de l'IA en particulier. Edmonds et al. estiment que cette évolution est le résultat d'un alignement croissant des intérêts et des préoccupations en matière de sécurité, fondé sur la perception commune que la Russie et la Chine sont en concurrence avec les États-Unis qui ont mis en place sanctions, contrôles à l'exportation et droits de douane¹⁰⁵ pour se protéger.

Le chapitre suivant présente les accords qui sous-tendent la coopération sino-russe en matière de technologie et d'innovation avant de décrire les différents domaines de coopération entre les deux pays. La coopération industrielle entre les entreprises chinoises et russes est ensuite analysée, en mettant l'accent sur les activités de Huawei en Russie. Enfin, le dernier point traité aborde les limites de la coopération russo-chinoise en matière d'intelligence artificielle.

4.1 Accords sous-tendant la coopération technologique entre la Russie et la Chine

La technologie et l'innovation occupent une place de plus en plus importante dans le partenariat stratégique entre la Chine et la Russie. Depuis la visite d'État de Xi Jinping à Moscou en mai 2015, les deux gouvernements ont signé plusieurs accords visant à étendre leur coopération à de nouveaux domaines dont l'économie numérique. Le Ministère de la science et de la technologie chinois et le Ministère russe du développement économique ont notamment signé en juin 2016 un « protocole

¹⁰² Edmonds et al, 2021, p. 103

¹⁰³ Morgan et al, 2020, p. 88-89

¹⁰⁴ Edmonds et al, 2021, p. 153-156

¹⁰⁵ Edmonds et al, 2021, p. 153-159



d'accord sur le lancement de la coopération dans le domaine de l'innovation ». En outre, dans le cadre du « partenariat stratégique global » que la Russie et la Chine ont annoncé en 2019, l'idée que les deux nations sont liées par un "partenariat de coopération scientifique et technologique pour une innovation partagée" est devenue l'un des piliers de la relation¹⁰⁶.

Bien que cette notion ait été essentiellement de façade, les deux gouvernements ont lancé de nouveaux forums et mis en place des mécanismes pour promouvoir une collaboration plus approfondie, notamment des projets conjoints et des partenariats entre entreprises. La coopération technologique entre la Russie et la Chine a gagné en substance au fil du temps et s'est de plus en plus institutionnalisée. Les deux pays collaborent sur un certain nombre de technologies, parmi lesquelles, l'intelligence artificielle et la robotique constituent des priorités¹⁰⁷.

Actuellement, les revenus que la Russie tire de l'activité liée à l'IA augmentent dix fois plus vite que le PIB du pays. Toutefois, ces statistiques sont négligeables par rapport aux chiffres chinois, où les investissements dans la recherche sur l'IA sont 350 fois plus importants qu'en Russie. En outre, la Chine est le deuxième pays, après les États-Unis, pour le nombre de personnes employées dans le secteur. Ce n'est là qu'un des nombreux domaines dans lesquels les deux pays ont des intérêts et des opportunités communs.

4.2 Domaines de coopération technologique entre la Russie et la Chine

Dans un rapport de 2019, Bendett et Kania décrivent cinq domaines dans lesquels les relations sino-russes s'approfondissent : les dialogues et échanges, les fonds d'investissement conjoints, le développement de parcs industriels scientifiques et technologiques, les concours conjoints et l'expansion de la coopération universitaire¹⁰⁸.

Le forum d'échange le plus important entre la Russie et la Chine en matière de technologie est le Dialogue sino-russe sur l'innovation. Celui-ci a lieu chaque année depuis 2017 et est organisé conjointement par le Ministère de la Science et de la Technologie chinois et le Ministère russe du Développement économique. Sa première édition en 2017 avait rassemblé plus de 100 entreprises chinoises et russes issues de divers secteurs comme les nanotechnologies, la robotique et l'IA. Par ailleurs, la Russie et la Chine ont signé en 2018, un plan de coopération russo-chinois en matière d'innovation pour la période 2019-2024¹⁰⁹.

La Russie et la Chine ont ouvert un premier parc scientifique et technologique commun en 2006 dans la ville chinoise de Changchun. En juin 2016, elles ont déclaré travailler sur le projet de parc d'innovation Chine-Russie, situé dans la province chinoise du Shanxi et financé par le gouvernement provincial, le Fonds d'investissement direct russe et le Fonds d'investissement sino-russe. Lors de son ouverture en 2018, des entreprises informatiques, biomédicales et d'IA ont été invitées à y participer. Par ailleurs, en 2017, les parcs scientifiques et technologiques de Chine et de Russie ont

¹⁰⁶ Bendett & Kania, 2019, p. 5

¹⁰⁷ Bendett & Kania, 2019, p. 5, 9-10

¹⁰⁸ Bendett & Kania, 2019, p. 5-8

¹⁰⁹ Bendett & Kania, 2019, p. 5

annoncé œuvrer à l'élaboration d'un centre de haute technologie sino-russe dans le parc technologique de Skolkovo. En 2018, les autorités de la ville chinoise de Harbin, située à proximité de la frontière russe, ont dévoilé un projet visant à faire de la localité un centre de coopération technologique sino-russe¹¹⁰.

Parallèlement, la Russie et la Chine ont également investi de plus en plus de fonds dans la R&D, et plus particulièrement dans le secteur des technologies de pointe, e.g. le Fonds d'investissement Russie-Chine pour le développement régional est devenu en 2018 un investisseur de référence pour deux nouveaux fonds de Skolkovo Ventures pour 283 millions d'euros (300 millions de dollars américains). Plus significative est la création en juillet 2019 d'un Fonds d'investissement conjoint sino-russe pour l'innovation doté d'un budget initial de 943,4 millions d'euros (1 milliard de dollars américains). Ce fonds, financé par le Fonds russe d'investissement direct et la Coopération chinoise d'investissement est, entre autres, amené à être consacré au financement de la recherche en IA¹¹¹.

La coopération entre les secteurs technologiques chinois et russe a également été encouragée par le biais de concours et de compétitions. En septembre 2018, le premier concours d'innovation industrielle sino-russe a ainsi été organisé. Il s'est focalisé sur les *big data*, l'IA et la fabrication industrielle de pointe. En juillet 2018, des institutions universitaires russes et chinoises ont également signé un accord incluant une feuille de route pour développer les « fonctions cérébrales » comprenant des éléments d'IA¹¹².

4.3 Évolution de la coopération industrielle et du rôle de Huawei en Russie

Huawei a joué un rôle capital dans la coopération commerciale entre la Russie et la Chine en matière de haute technologie et notamment d'IA. L'entreprise a ouvert ses premiers instituts de recherche à Moscou et à Saint-Petersbourg en 2017. Ces derniers se focalisent sur le développement de modèles mathématiques pour les technologies de communication. Leur ouverture a été suivie en 2019, après que l'entreprise ait exprimé sa volonté de tripler son personnel de R&D en Russie, de celle de trois centres supplémentaires. En juin 2019, Huawei a obtenu la licence lui permettant d'exploiter la technologie de reconnaissance faciale développée par la *start-up* russe Vocord pour un montant déclaré de 47 millions d'euros (50 millions de dollars américains). L'entreprise chinoise a par ailleurs signé un accord de coopération avec Skolkovo et, en novembre 2019, annoncé son intention de construire d'ici 2025 un écosystème d'IA en Russie composé de 20 universités, de plus de 100 entreprises de logiciels et de plus de 100 000 développeurs d'IA¹¹³.

Huawei Technologies Co. Huawei Holding & Investment Co.	
Structure de l'entreprise et actionnaires ¹¹⁴	Huawei Technologies Co, Ltd. Huawei Technologies Co. est une filiale de Huawei Holding & Investment Co. et est détenue à 100 % par cette dernière.

¹¹⁰ Bendett & Kania, 2019, p. 6 ; Edmonds et al, 2021, p. 160

¹¹¹ Bendett & Kania, 2019, p. 7 ; Edmonds et al, 2021, p. 160

¹¹² Bendett & Kania, 2019, p. 7

¹¹³ Edmonds et al, 2021, p. 161, Simes, 2020

¹¹⁴ Huawei, 2022, p. 152-157

	Huawei Holding & Investment Co. Ltd. • Ren Zhengfei (fondateur et PDG) : ~1 %. • Union de Huawei Investment & Holding Co, Ltd : ~99%.
Les dirigeants ¹¹⁵	• Président du conseil d'administration : Liang Hua • Fondateur et PDG : Ren Zhengfei • Vice-présidente du conseil d'administration et directrice financière : Meng Wanzhou (fille de Ren Zhengfei)
Beijing et Huawei ?	
Selon le rapport annuel de <i>Huawei Investment & Holding Co. Ltd</i>, Huawei est une « société privée entièrement détenue par ses employés <i>Huawei Investment & Holding Co. Ltd</i>, qui est la société mère de Huawei Technologies Co. Ltd, n'a que deux actionnaires : Ren Zhengfei, fondateur de Huawei, et l'<i>Union of Huawei Investment & Holding Co. Ltd</i>. Par l'intermédiaire de cette dernière, Huawei met en œuvre un « plan d'actionnariat salarié », auquel 131 507 employés actuels ou retraités participaient au 31 décembre 2021. L'Union exerce ses droits d'actionnaire par l'intermédiaire de la Commission des représentants qui élit le conseil d'administration et le conseil de surveillance de Huawei. La Commission des représentants compte 115 membres, qui sont élus par les « salariés actionnaires disposant de droits de vote » sur la base d'un vote par action¹¹⁶. Toutefois, les salariés de Huawei ne possèdent pas d'actions réelles de Huawei Technologies ou de Huawei Holding & Investment, mais seulement une sorte d'« action virtuelle » qui leur permet de participer aux bénéfices¹¹⁷. Ils décrivent donc le « système d'actionnariat salarié » comme « un simple système d'incitation à la participation aux bénéfices »¹¹⁸. Étant donné qu'en Chine, les syndicats sont responsables devant des organisations syndicales supérieures - théoriquement jusqu'à la Fédération chinoise des syndicats, qui est contrôlée par le PCC – selon Christopher Balding et Donald C. Clarke Huawei peut être considérée comme une entreprise publique¹¹⁹. Huawei a publiquement rejeté les allégations d'être une entreprise étatique en déclarant que la Commission des représentants, qui est distincte du comité syndical, était l'autorité suprême de l'entreprise¹²⁰.	

Les projets de coopération de Huawei font partie d'une stratégie plus large pour le marché russe appelée « TIGER ». Dans le cadre de cette stratégie, Huawei se concentre sur le développement du système d'IA russe. Elle prévoit ainsi d'utiliser son laboratoire d'innovation Huawei OpenLab inauguré à Moscou en 2018 pour renforcer la coopération avec les entreprises russes. Elle devrait en même temps former des développeurs russes dans le cadre de sa communauté mondiale de développement Ascend. Enfin, elle projette de développer des cours liés aux technologies d'IA en collaboration avec les universités russes. Selon Edmonds et al, l'entreprise aurait investi 4,7 millions d'euros (5 millions de dollars américains) dans des partenariats en Russie en 2020 et prévoirait à la

¹¹⁵ Huawei, 2020, p. 152-157

¹¹⁶ Huawei, 2022, p. 152

¹¹⁷ Balding & Clarke, 2019, p. 5

¹¹⁸ Balding & Clarke, 2019, p. 5

¹¹⁹ Balding & Clarke, 2019, p. 10-11

¹²⁰ Li, 2019

fois d'augmenter ses achats auprès de fournisseurs russes¹²¹ et d'augmenter le nombre de centres de R&D en Russie pour le porter à cinq¹²².

En 2020, l'Institut de recherche russe de Huawei (une entité séparée d'OpenLab : <https://career.huawei.ru/rri/en/>) a créé un laboratoire de R&D commun pour l'IA et l'apprentissage profond avec l'École de mathématiques appliquées et d'informatique de l'Institut de physique et de technologie de Moscou. Le laboratoire se concentre sur « le développement d'algorithmes de réseaux neuronaux pour la vision par ordinateur, l'apprentissage automatique et l'IA ; le développement de méthodes pour la photographie computationnelle et l'amélioration des images à l'aide de la modélisation mathématique et d'algorithmes avancés ; et la résolution de problèmes complexes afin de créer des algorithmes pour la recherche et le positionnement simultanés¹²³ ». Ce laboratoire qui est le dixième laboratoire mis en place par Huawei en collaboration avec des universités et des instituts de recherche russes, ne devrait pas être le dernier puisque l'entreprise prévoit de collaborer avec d'autres institutions universitaires russes par le biais de financements et de partenariats¹²⁴.

Huawei a également conclu des partenariats commerciaux avec des entreprises russes. Elle travaille ainsi avec la *start-up* russe VisionLabs dont elle sollicite l'expertise en matière de vision artificielle pour l'apprentissage automatique (dans les produits Huawei Atlas). Au-delà de l'IA, Huawei collabore également avec des entreprises russes dans le domaine du « *cloud computing* » : elle est partenaire avec la société russe de cybersécurité Kaspersky dont elle utilise la plateforme FusionSphere. Par ailleurs, Huawei a signé en mars 2020, un contrat avec Sberbank pour lancer une coentreprise ciblant le marché russe de la 5G. Baptisée SberCloud.Advanced, cette dernière témoigne de l'investissement de l'acteur dans le développement de l'écosystème technologique russe¹²⁵.

Toutefois, l'invasion russe de l'Ukraine le 24 février 2022 et l'imposition subséquente de sanctions strictes contre la Russie par les États-Unis et l'Union européenne ont affecté les activités de Huawei en Russie. En décembre 2022, le journal russe *Kommersant* a rapporté que Huawei démantèlerait le 1er janvier 2023 sa division *Russian enterprise business group*, chargée de vendre des systèmes de stockage de données et des équipements de télécommunications aux entreprises russes, afin d'éviter le risque de sanctions secondaires. Les quelques 2 000 employés de la filiale seront déplacés vers d'autres pays « post-soviétiques » ou licenciés. Les centres de R&D de Huawei à Moscou, Saint-Petersbourg, Nijni Novgorod et Novossibirsk seront quant à eux maintenus dans leur forme actuelle¹²⁶.

¹²¹ De 370 millions d'euros (soit 392 millions de dollars américains) entre 2017 et 2019, ces derniers passeraient à 755 millions d'euros (800 millions de dollars américains) entre 2020 et 2025

¹²² Edmonds et al, 2021, p. 161-162

¹²³ Edmonds et al, 2021, p. 162

¹²⁴ Edmonds et al, 2021, p. 162

¹²⁵ Edmonds et al, 2021, p. 163, Nocetti, 2020, p. 42

¹²⁶ Deng, 2022

Outre Huawei, d'autres entreprises chinoises collaborent avec des sociétés russes dans le domaine de l'IA. C'est le cas de la société chinoise Dahua Technology et de la *start-up* russe NTechLab qui ont présenté en mai 2019 une caméra dotée de capacités de reconnaissance faciale qu'elles ont mis au point conjointement¹²⁷. Le logiciel de reconnaissance faciale développé par NTechLab a été intégré au réseau de caméras de surveillance de la ville de Moscou¹²⁸. Initialement destiné à faciliter les enquêtes policières, le logiciel a été utilisé durant la période de pandémie de Covid-19 pour identifier les personnes contrevenant à la quarantaine et pourrait probablement être à l'avenir employé par le contre-espionnage¹²⁹.

Par ailleurs, la société de logiciels chinoise Vinci Group (différent du groupe français du même nom), a conclu un accord avec la *start-up* informatique russe Jovi Technologies pour travailler sur des produits d'IA¹³⁰.

NtechLab	
Structure de l'entreprise, actionnaires et investisseurs	Les actionnaires¹³¹ - Fondateurs de l'entreprise : actionnaires majoritaires - Rostec State Corporation : 12,5% + 1 action (Note : selon un rapport du magazine américain Wired, Rostec a vendu sa participation minoritaire entre-temps).¹³² - Vardanyan, Broitman and Partners (VB Partners) : 25% + 1 action (société d'investissement privée qui gère les actifs de Ruben Vardanyan et de ses partenaires)¹³³ - Impulse VC : participation minoritaire non divulguée¹³⁴ Autres investisseurs - Fonds russe d'investissement direct¹³⁵ - Mubadala Investment Company (fonds national des Émirats arabes unis)¹³⁶
Les fondateurs	- Alexander Kabakov - Artem Kuharenko

¹²⁷ Nocetti, 2020, p. 41

¹²⁸ Edmonds et al, 2021, p. 69-70

¹²⁹ Edmonds et al, 2021, p. 69-70

¹³⁰ Edmonds et al, 2021, p. 164

¹³¹ Rostec, 2018

¹³² Borak, 2023

¹³³ Vardanyan, Broitman and Partners, s.d.

¹³⁴ "Un milliardaire russe investit dans la technologie de reconnaissance faciale", 2017

¹³⁵ Brewster, 2020

¹³⁶ Brewster, 2020

	Note : Selon un rapport du magazine américain Wired, Alexander Kabakov et Artem Kuharenko ont tous deux quitté le NTechLab et la Russie en décembre 2021 et février 2022, déclarant leur position anti-guerre sur les médias sociaux ¹³⁷ .
--	---

Zhejiang Dahua Technology Co, Ltd (Dahua Technology)¹³⁸	
Structure de l'entreprise et actionnaires	• Coté à la bourse de Shenzhen Principaux actionnaires • Fu Liquan (fondateur) : 13,37% • Shanghai Gaoyi Investment Management Co. Ltd : 7,21 %. • Zhu Jiangming (Vice-président exécutif) : 2,10% • China Securities Finance Corp. Ltd : 2,07% • Chen Ailing (épouse de Fu Liquan) : 0,93%
Les dirigeants	• Président du conseil de surveillance : Song Maoyuan • Président et directeur : Li Ke

4.4 Limites de la coopération entre la Russie et la Chine

Si les chapitres précédents ont démontré que la coopération sino-russe dans les domaines de la haute technologie et de l'IA s'est intensifiée ces dernières années, Bendett et Kania notent les limites de la coopération sino-russe : les importants problèmes de confiance dans la propriété intellectuelle subsistent entre les deux acteurs et empêchent la Russie d'adopter ou d'acquérir des produits chinois de haute technologie¹³⁹. Néanmoins, si les Russes se plaignent depuis longtemps du vol de leur propriété intellectuelle par les acteurs chinois¹⁴⁰, les préoccupations en la matière ne semblent pour l'heure pas prévaloir. Les Russes paraissent davantage préoccupés par la fuite de leurs « cerveaux » vers la Chine¹⁴¹. Le président de l'Académie russe des sciences a ainsi en 2019 publiquement exprimé ses inquiétudes quant au fait que la Chine attirait les talents russes dans le domaine des sciences « STEM » (*science, technology, engineering and mathematics*) en leur offrant de meilleurs salaires et conditions de travail¹⁴². Outre la réappropriation de la propriété intellectuelle et la captation du capital humain, les dirigeants russes semblent également s'inquiéter de la fuite de données de la Russie vers la Chine¹⁴³.

¹³⁷ Borak, 2023

¹³⁸ Factiva, 2023

¹³⁹ Bendett & Kania, 2019, p. 14

¹⁴⁰ Nocetti, 2020, p. 43

¹⁴¹ Bendett & Kania, 2019, p. 14

¹⁴² Bendett & Kania, 2019, p. 14

¹⁴³ Nocetti, 2020, p. 43

Ces préoccupations sont néanmoins relativisées par la question de l'asymétrie technologique croissante entre les deux pays. Les élites russes ne croient pas que la Chine considère la Russie comme un partenaire en matière d'IA et de haute technologie¹⁴⁴. Parallèlement, une partie de l'élite russe considère la Chine comme un modèle pour la Russie en ce qui concerne l'utilisation de l'IA et d'autres technologies à des fins de contrôle et de surveillance de masse¹⁴⁵. Néanmoins, selon Julien Nocetti, les experts russes estiment que le partage des innovations de l'IA dans le domaine militaire dépassent les limites de la confiance de la coopération sino-russe¹⁴⁶. Les limites cependant remettent en cause compte tenu de la réalité de la guerre avec l'Ukraine et des sanctions occidentales.

Étant donné que les grandes entreprises technologiques chinoises telles que Huawei ont réduit leurs exportations vers la Russie par crainte de sanctions secondaires de la part des États-Unis, les entreprises technologiques russes doivent de plus en plus compter sur des composants et des équipements de qualité inférieure produits par des fabricants chinois de deuxième et de troisième rangs.

5. Étude de cas : Covid-19 et la surveillance de masse

Comme indiqué dans la section précédente, une partie de l'élite russe considère que la Chine pourrait servir de modèle à son pays en ce qui concerne l'utilisation de l'IA et d'autres technologies pour le contrôle et la surveillance de masse. Les mesures sanitaires adoptées par les deux pays pendant la période de pandémie de Covid-19 constituent une étude de cas utile pour démontrer le degré auquel la Russie a commencé à suivre le modèle chinois de contrôle des masses, et les répercussions que ce choix a engendré sur l'effort de guerre russe actuel. Ce chapitre analyse l'utilisation chinoise et russe des outils de surveillance numérique pendant la pandémie de Covid-19 avant de décrire la manière dont la Russie emploie ses réseaux de surveillance numérique pour surveiller et mobiliser massivement depuis le déclenchement de la guerre en Ukraine.

5.1 Surveillance de masse et mesures Covid-19 en Chine

Avant la pandémie de Covid-19, la Chine possédait déjà le plus grand réseau de surveillance au monde, composé de multiples réseaux locaux dotés de centaines de millions de caméras¹⁴⁷. La Chine a notamment déployé des systèmes de surveillance incluant des technologies de reconnaissance faciale dans la région autonome ouïgoure du Xinjiang, dans laquelle plus de 170 millions de caméras auraient été utilisées en 2018¹⁴⁸. De plus, le gouvernement chinois a déployé de grands efforts pour développer un¹⁴⁹ système de crédit social, qui permet via une notation de récompenser ou sanctionner les citoyens, les entreprises et les organismes gouvernementaux en fonction de leur comportement¹⁵⁰.

¹⁴⁴ Nocetti, 2020, p. 43 ; Simes, 2020

¹⁴⁵ Nocetti, 2020, p. 43

¹⁴⁶ Nocetti, 2020, p. 43

¹⁴⁷ Khalil, 2020, p. 10

¹⁴⁸ Lo, 2022, p. 1

¹⁴⁹ Khalil, 2020, p. 11

¹⁵⁰ Khalil, 2020, p. 11-12

La pandémie de Covid-19 et la réponse du Pékin en matière de gestion des urgences ont mis en évidence ce système de surveillance numérique, qui combine technologie de reconnaissance faciale, caméras de sécurité dans les espaces publics et fermés, surveillance des médias sociaux, traçage des télécommunications et suivi des informations numériques sur les voyageurs. La pandémie a permis à la Chine d'étendre l'utilisation des technologies de surveillance au niveau national. Des caméras de surveillance supplémentaires ont été installées devant les portes d'entrée des maisons voire même à l'intérieur des immeubles résidentiels. La Chine a déployé des scanners thermiques et des outils de reconnaissance faciale dans les gares et autres lieux publics. La pandémie a également encouragé le développement de nouveaux outils de surveillance comme par exemple, ceux de l'entreprise *KC Wearable* qui a mis au point des « casques intelligents » afin de détecter la température corporelle, scanner les codes QR pour obtenir des données personnelles, reconnaître les plaques d'immatriculation et identifier les personnes à l'aide d'un logiciel de reconnaissance faciale¹⁵¹.

Pendant cette période, la Chine a également utilisé une application de suivi des contacts, « Health Code », qui est parfaitement intégrée dans des applications mobiles grand public telles que WeChat et Alipay¹⁵². Cette application attribue aux utilisateurs un code QR de couleur (vert, jaune ou rouge), indiquant si une personne peut ou non voyager ou accéder à des lieux publics¹⁵³. Ce code coloré est calculé en fonction des réponses à un questionnaire portant sur les antécédents de voyage et de santé.¹⁵⁴ Parallèlement, le gouvernement chinois a mis en place une « carte de voyage *big data* » utilisant les données mobiles des trois plus grandes sociétés de télécommunications (China Telecom, China Mobile et China Unicom) pour suivre l'historique des déplacements de chaque personne au cours des quatorze derniers jours¹⁵⁵. Les informations de la carte de voyage sont connectées avec les codes QR de santé, permettant aux autorités de recouper les deux sources de données et ainsi éviter les informations erronées ou falsifiées. De nombreux autres pays ont utilisé des applications de suivi des contacts pour lutter contre la pandémie de Covid-19, mais l'application chinoise « Health Code » a atteint un niveau de précision plus élevé en collectant automatiquement de très nombreuses informations personnelles¹⁵⁶.

Khalil conclut que la pandémie a permis aux autorités chinoises de démontrer le fonctionnement des technologies de surveillance et son efficacité concrète à grande échelle (?) en situation d'urgence¹⁵⁷. En outre, Lo affirme¹⁵⁸ que la pandémie de Covid-19 aurait changé la vision de la population concernant la surveillance, et conduit au développement d'une « culture de la surveillance », l'acceptation de laquelle parmi les citoyens chinois dépend de leur niveau de

¹⁵¹ Khalil, 2020, p. 14-17

¹⁵² Lo, 2022, p. 1

¹⁵³ Lo, 2022, p. 1

¹⁵⁴ Xu & Liu, 2021, p. 33

¹⁵⁵ Xu & Liu, 2021, p. 33

¹⁵⁶ Lo, 2022, p. 1

¹⁵⁷ Khalil, 2020, p. 19

¹⁵⁸ Lo, 2022, p. 3

l'information sur son potentiel répressif par le traçage des contacts et par la surveillance des personnes.¹⁵⁹

5.2 Surveillance de masse et mesures Covid-19 en Russie

Avant la période de pandémie de Covid-19, les autorités russes avaient pris leurs dispositions pour mettre en place des systèmes de surveillance à grande échelle. Moscou a ainsi servi de terrain d'essai pour les technologies de gestion des villes numériques. Dès 2018, le Département des technologies de l'information (DIT) de la capitale a présenté sa stratégie numérique pour la ville, « Smart City 2030 ». L'utilisation de l'IA pour analyser des données provenant de diverses sources et fournir des solutions au gouvernement et aux entreprises est un élément clé de cette stratégie. Pour fournir des données sur les déplacements des habitants de Moscou, le DIT achète depuis 2015 des données aux opérateurs de téléphonie mobile, y compris des données SIM et de suivi, tout en utilisant également des données provenant des cartes de transport du métro de Moscou, des historiques des courses de taxis, des images provenant de caméras (photo et vidéo), ainsi que des données provenant de réseaux Wi-Fi publics. Bien que l'adjoint au maire de Moscou, Maxim Liksutov, ait affirmé que la ville n'avait traité que des données anonymisées, certains craignent que ces données puissent être utilisées pour suivre les déplacements de personnes spécifiques¹⁶⁰.

Dans le même temps, la mairie de Moscou a progressivement installé un système de vidéosurveillance à grande échelle. Le système comptait 178 000 caméras au début de l'année 2020, un nombre qui reste toutefois modeste en comparaison aux normes mondiales. À partir de 2017, un système de reconnaissance faciale utilisant l'IA et le logiciel FindFace de la société russe NTechLab a été intégré au système de vidéosurveillance. À l'origine, la mairie de Moscou a fait valoir que ce dernier répondait à des besoins de sécurité. La Coupe du monde 2018 a servi de premier test grandeur nature. D'après les autorités, pendant le tournoi, 180 délinquants répertoriés dans les bases de données fédérales auraient été arrêtés. Compte tenu de son efficacité, le système a par la suite été renforcé. En janvier 2020, il (le système de reconnaissance faciale) comprenait 105 000 caméras « intelligentes »¹⁶¹.

La pandémie de Covid-19 a permis aux autorités moscovites de tester et d'améliorer leur système de contrôle numérique. À la fin de la période de confinement, il fonctionnait sans problème majeur¹⁶². À la mi-mars 2020, les autorités ont commencé à surveiller les cartes SIM des personnes qui rentraient en Russie et à leur envoyer des SMS leur demandant de rester chez elles¹⁶³. Le 29 mars, le maire de Moscou, Sergey Sobyannin, a étendu ce contrôle à tous les habitants de la ville¹⁶⁴. Pour le faire respecter, il a mis en place le 15 avril 2020 un système de laissez-passer numérique : Pour quitter leur domicile, les Moscovites devaient s'inscrire sur un site web ou une application du gouvernement et déclarer un itinéraire et un but. Ils recevaient ensuite un QR code qui pouvait être

¹⁵⁹ Xu Xu, 2022

¹⁶⁰ Markotkin, 2021, p. 1-2

¹⁶¹ Markotkin, 2021, p. 2-3

¹⁶² Markotkin, 2021, p. 3

¹⁶³ Markotkin, 2021, p. 3

¹⁶⁴ Markotkin, 2021, p. 3

vérifié par les autorités¹⁶⁵. Après avoir mis en place ce système à Moscou, le gouvernement russe a décidé de l'étendre à tout le pays¹⁶⁶. Le 23 avril, le DIT de Moscou lançait ainsi une application de « suivi social » pour surveiller les personnes infectées non hospitalisées¹⁶⁷.

Au plus fort de la pandémie de Covid-19, les autorités de Moscou ont lancé le réseau de surveillance « Safe City » qui s'appuie sur le réseau existant de caméras de surveillance de Moscou. Outre les informations collectées par plus de 200 000 caméras, Safe City utilise des données provenant de 169 systèmes d'information, parmi lesquelles des données de géolocalisation anonymisées fournis par les téléphones portables, des données provenant de services de covoiturage et des dispositifs de reconnaissance vocale. À la mi-mars 2020, le système de reconnaissance faciale de « Safe City » aurait détecté 200 personnes enfreignant les restrictions liées au confinement. Encouragé par ces premiers résultats, le gouvernement russe a annoncé son intention d'investir environ 1,2 milliard d'euros¹⁶⁸ pour déployer des systèmes similaires dans toute la Russie, alors même que « Safe City » était encore en cours de déploiement à Moscou¹⁶⁹. Dans le même temps, Rostec aurait travaillé à l'extension du projet « Safe City » en développant un logiciel destiné à aider les autorités à anticiper les émeutes et à prévenir leur escalade en analysant les informations publiées dans les médias, les données des réseaux sociaux, les caméras de surveillance et d'autres sources¹⁷⁰.

Après la levée de la plupart des restrictions liées à la pandémie, des éléments clés de la surveillance numérique, notamment le système de reconnaissance faciale et l'utilisation des données de géolocalisation pour suivre les mouvements des personnes, ont été maintenus¹⁷¹. M. Barros¹⁷² affirme que, convaincu de leur utilité depuis l'expérience du printemps 2020, le Kremlin s'efforce d'étendre les outils de contrôle à l'ensemble du pays. Pendant le confinement, le rôle de Moscou en tant que terrain d'essai pour les technologies numériques a été renforcé après que la Douma, la chambre basse du parlement russe, ait en avril 2020 adopté une loi fédérale créant les conditions nécessaires au développement et à la mise en œuvre des technologies de l'IA à Moscou¹⁷³. La nouvelle loi a mis en place un cadre juridique expérimental - un bac à sable réglementaire - pour le développement d'applications d'IA exemptant les autorités des contraintes légales relatives à la protection des données¹⁷⁴. Par ailleurs, le 8 juin 2020, Vladimir Poutine a promulgué une loi établissant un registre unifié d'informations sur les citoyens russes, qui comprend, entre autres, les informations indiquées sur le passeport, dans l'état civil, sur les fiches d'imposition et les livrets familiaux¹⁷⁵. Les défenseurs des droits numériques russes ont décrit la création de ce système

¹⁶⁵ Ilyushina, 2020

¹⁶⁶ Barros, 2020

¹⁶⁷ Markotkin, 2021, p.3

¹⁶⁸ Conversion des roubles en euros en utilisant le taux de change annuel moyen en 2020 de 1 € = 82,73 roubles.

¹⁶⁹ Borak, 2023

¹⁷⁰ Borak, 2023

¹⁷¹ Markotkin, 2021, p. 4

¹⁷² Barros, 2020

¹⁷³ Markotkin, 2021, p. 2, Borak, 2023

¹⁷⁴ Markotkin, 2021, p. 2 ; Borak, 2023

¹⁷⁵ Barros, 2023

comme une tentative d'obtenir un « monopole presque illimité » sur la collecte et le stockage des données biométriques¹⁷⁶.

5.3 Surveillance de masse en Russie dans le contexte de la guerre en Ukraine

Pour répondre aux manifestations contre la guerre en Ukraine, le Kremlin a donc pu s'appuyer sur un système de surveillance numérique testé et approuvé. En examinant plus de 2000 affaires judiciaires, l'agence de presse Reuters a découvert que le réseau de vidéosurveillance à reconnaissance faciale de Moscou a joué un rôle important dans l'arrestation de centaines de manifestants, arrêtés pour la plupart suite aux manifestations antigouvernementales en 2021. Depuis le début de l'invasion de l'Ukraine, les autorités russes utilisent la reconnaissance faciale pour empêcher les gens de manifester. Selon les données du groupe russe de défense des droits de l'homme OVD-Info, en 2022, au moins 141 personnes ont été arrêtées à titre préventif grâce à la reconnaissance faciale. Elles ont notamment été interpellées par la police dans les stations de métro de Moscou les jours fériés, en prévision de manifestations ou encore à des moments où le sentiment anti-guerre était élevé. Dans le cadre de son système de paiement, le métro de Moscou utilise également un système de reconnaissance faciale baptisé « Sfera ».

Selon un communiqué de presse publié en 2021 sur le site web de la ville de Moscou, le métro a fait appel à trois entreprises russes pour optimiser son système de reconnaissance faciale baptisé Sfera¹⁷⁷. Ces dernières sont NTechLab, VisionLabs (dont le siège se trouve aux Pays-Bas mais qui appartient au plus grand opérateur de téléphonie mobile de Russie, MTS), et Tevian (une société d'IA fondée par des chercheurs de l'Université d'État de Moscou). Les contrats publiés en 2022 sur le site web des appels d'offres de l'État russe montrent que le système de reconnaissance faciale de Moscou s'appuie sur quatre logiciels : LunaPlatform de VisionLabs, FindFace de NTechLab, FaceSDK de Tevian et un logiciel de reconnaissance faciale appelé Kipod, développé par une société biélorusse, Synesis visée par les sanctions occidentales en raison du rôle qu'elle a joué dans la répression des mouvements pro-démocratiques au Belarus et en Russie¹⁷⁸.

Selon Reuters, ces entreprises ont utilisé des technologies américaines dans leurs logiciels. NTechLab et VisionLabs emploient ainsi des processeurs graphiques (GPU) de la société américaine Nvidia tandis que Synesis recourt à des unités centrales (CPU) d'Intel. Nvidia et Intel affirment avoir interrompu leurs ventes à la Russie et au Belarus depuis le début de l'invasion de l'Ukraine en février 2022. Toutefois, selon les registres des douanes russes, au moins 129 cargaisons de produits Nvidia auraient été importées en Russie entre le 1er avril et le 31 octobre 2022. Parmi ces dernières, au moins 57 contenaient des GPU¹⁷⁹. De même, des produits Intel d'une valeur d'au moins 431 millions d'euros (457 millions de dollars) auraient été importés en Russie entre le 1er avril et le 31 octobre 2022. Selon une enquête conjointe de Reuters et du groupe de réflexion RUSI, des composants informatiques et électroniques occidentaux visés par les sanctions, continuent d'être importés en Russie via des intermédiaires à Hong Kong, en Turquie et en Chine¹⁸⁰.

¹⁷⁶ Borak, 2023

¹⁷⁷ Masri, 2023

¹⁷⁸ Masri, 2023

¹⁷⁹ Masri, 2023

¹⁸⁰ Stecklow, Gauthier-Villars et Tamman, 2022

5.4 Comparaison de la surveillance de masse en Chine et en Russie

Comparer les mesures prises en urgence en Russie et en Chine lors de la pandémie de Covid-19 permet de constater qu'il existe de nombreux points communs entre les deux pays. Dans chacun d'eux, les autorités se sont fortement appuyées sur les technologies numériques pour faire appliquer les mesures sanitaires. Les systèmes de vidéosurveillance à grande échelle dotés de capacités de reconnaissance faciale basées sur l'IA ont joué un rôle clé. Les deux pays ont profité de la pandémie pour étendre les champs d'utilisation des systèmes de surveillance de masse. Néanmoins, il convient de noter que la quantité et la densité des caméras de surveillance déployées en Russie étaient et restent sans commune mesure avec celles mises en place en Chine. En Russie, les systèmes de surveillance à grande échelle n'ont été installés qu'à Moscou, qui sert de laboratoire pour les technologies numériques. Toutefois, lors de la première vague de la pandémie, au printemps 2020, le gouvernement russe a pris des mesures visant à étendre à d'autres villes les outils numériques, e.g. les QR codes, les réseaux de vidéosurveillance. En conclusion, la pandémie de Covid-19 semble avoir convaincu les responsables russes - - qu'une surveillance à grande échelle est à la fois possible et efficace. Il n'est donc pas surprenant que la surveillance numérique ait eu une importance décisive dans les tentatives du Kremlin pour étouffer les manifestations au début de l'invasion russe de l'Ukraine.

En avril 2023, le gouvernement russe a fait adopter à la hâte par le Parlement une loi autorisant les autorités à émettre les ordres de mobilisation par voie électronique, via le site web des services de l'État Gosuslugi et à constituer une base de données répertoriant tous les Russes éligibles au service militaire. Si un ordre de mobilisation est émis et qu'une personne ne se présente pas au bureau de recrutement, elle peut être sanctionnée. Les sanctions comprennent l'interdiction de quitter le territoire, de conduire, d'acheter et de vendre des biens immobiliers, de contracter des prêts et d'enregistrer une petite entreprise. En d'autres termes, le système de contrôle numérique ferme effectivement les frontières de l'État à des centaines de milliers d'individus susceptibles d'être mobilisés. Pendant ce temps, cette nouvelle base de données recueillera des informations sur les appelés potentiels à partir de toutes les sources disponibles, y compris les dossiers médicaux et électoraux, les tribunaux et les déclarations d'impôts. Selon Tatiana Stanovaya¹⁸¹, ce nouveau système est un premier pas vers l'établissement d'un système numérique de contrôle sociétal, qui réglemente l'accès des individus aux droits et aux avantages sur la base de leur loyauté politique.

Au sein du gouvernement russe, le Ministère du développement numérique sera chargé de créer le registre numérique prévu par cette nouvelle loi. Selon le site d'information Meduza, le Ministère du développement numérique chargera RT Labs, une filiale de Rostelecom aux liens étroits avec les autorités russes (le Ministre russe du développement numérique, Maksut Shadayev, est l'ancien PDG de RT Labs tandis que l'actuel PDG de RT Labs, Tengiz Alania, a été directeur adjoint du Centre régional des technologies de l'information et de la communication de Moscou) de créer ce registre. Meduza précise que le FSB supervisera tous les travaux réalisés par le Ministère du développement numérique et Rostelecom¹⁸².

¹⁸¹ Stanovaya, 2023

¹⁸² "State Services R Us" - La construction d'un "goulag numérique" pour les Russes appelés sous les drapeaux se transforme en un véritable casse-tête pour l'entrepreneur informatique du gouvernement", 2023

6. Scénarios et recommandations

La rivalité systémique entre les États-Unis et la Chine risque de diviser le monde interconnecté et globalisé, renforçant la bipolarité émergente. La concurrence qui s'ensuivra dans tous les systèmes socio-économiques vitaux sera dominée par le pays qui parviendra le premier à maîtriser le domaine de l'IA. Bien que les États-Unis soient en compétition directe avec la Chine dans l'application de l'IA dans de nombreux domaines, y compris l'économie, la défense et la société, le modèle de gouvernance chinois crée un champ dans lequel les États-Unis, en raison de leur système politique radicalement différent, ont délibérément choisi de ne pas participer¹⁸³. L'IA sera un élément essentiel des futures technologies militaires, offrant un avantage significatif à ceux qui pourront la déployer à grande échelle. L'avènement des armes autonomes, des drones pilotés par l'IA, des technologies spatiales et satellitaires avancées, ainsi que des matériels et logiciels militaires perturbateurs, montre que la révolution numérique est un phénomène durable. Elle est sur le point de redéfinir la nature de la guerre, entraînant des effets d'entraînement sans précédent. Il est donc indéniable que la concurrence dans les technologies militaires utilisant l'IA influence profondément la compétition entre Washington et Pékin.

Compte tenu de l'émergence de la Chine en tant que marché domestique le plus étendu pour les applications d'IA¹⁸⁴, il incombe à Washington d'être le fer de lance d'une alliance solide avec des nations partageant de mêmes valeurs pour cultiver une alternative viable et créer un contrepoids substantiel face à la Chine dans cette course technologique. Les États-Unis s'appuieront fortement sur leurs alliés européens pour renforcer et diversifier leur expertise en IA, tout en cherchant à construire une alliance solide dans la région indopacifique pour y contrer l'empreinte technologique croissante de la Chine. Pour préserver leur avance sur le long terme, les États-Unis devront entretenir des partenariats durables avec des alliés fiables et engagés.

Deux scénarios distincts se profilent: le premier, pessimiste, prévoit un découplage technologique progressivement complet, tandis que le second, optimiste, envisage une coexistence systémique pacifique. Pékin se concentrant sur la promotion de partenariats et d'engagements centrés sur la Chine afin de soutenir sa croissance intérieure jusqu'à ce qu'elle puisse contrebalancer l'influence écrasante des États-Unis. Si les États-Unis ont historiquement joué un rôle central dans l'ascension de la Chine,¹⁸⁵ ils pourraient également provoquer son déclin en initiant un désengagement technologique.

Sur la base des facteurs accélérant le développement de l'IA, soit l'investissement, l'innovation et la mise en œuvre, le Global AI Index (2021) classe respectivement les États-Unis et la Chine à la première et deuxième place. Cet index révèle l'avènement d'une course féroce aux armements technologiques dans laquelle l'IA n'est plus simplement une technologie mais l'avenir de la

¹⁸³ Allison & Schmidt, 2020.

¹⁸⁴ Allison & Schmidt, 2020.

¹⁸⁵ Schell O. (2020, 3 avril) ; The Ugly End of Chimerica ; Foreign Policy.

<https://foreignpolicy.com/2020/04/03/chimerica-ugly-end-coronavirus-china-us-trade-relations/>

technologie même¹⁸⁶. L'entité qui s'imposera dans le domaine aura vraisemblablement une influence majeure sur les affaires mondiales, tant sur le plan économique que militaire. Les implications pour l'économie politique, les alliances militaires, les partenariats et l'impact sur les normes et les règles mondiales dépendront de la vitesse, de la portée et de l'ampleur des progrès réalisés dans le domaine technologique. Au fil du temps, on pourrait assister à l'émergence de deux réseaux distincts de chaînes d'approvisionnement, l'un gravitant autour des États-Unis et l'autre autour de la Chine¹⁸⁷. Comme le souligne Rajiv Malhotra dans son dernier ouvrage¹⁸⁸, l'IA est le levier stratégique que la Chine utilise pour devancer les États-Unis et dominer le monde. Il devient de ce fait, le moyen le plus recherché dans la course au *leadership* économique, politique et militaire.

En outre, les technologies perturbatrices peuvent non seulement renforcer le contrôle de l'État (notamment via la surveillance de masse), mais aussi déstabiliser les systèmes démocratiques ouverts en bouleversant les équilibres politiques fragiles. Les tensions entre la Chine et l'Inde brouillent la dynamique de sécurité préexistante dans la zone Indopacifique. Parmi les exemples de coopération régionales récemment constituées pour répondre au contexte, celle de la Chine avec le Pakistan et, à plus grande échelle, celle entre la Chine et la Russie (le *Dragonbear*)¹⁸⁹.

Les coopérations dans le domaine numérique qui pourraient émerger restent néanmoins incertaines. Dans une perspective d'escalade entre la Chine et l'Inde, les États-Unis saisiraient toutes les occasions qui se présenteraient pour soutenir New Delhi, tandis que la Russie chercherait à jouer un rôle de médiateur. La compétition géostratégique se jouera principalement en mer de Chine méridionale et dans l'océan Indien, accentuant, d'une part, les tensions entre les géants asiatiques et, d'autre part, la concurrence entre la Chine et les États-Unis. Le point culminant de la rivalité géostratégique entre la Chine et l'Inde reste indéterminé. L'approche des deux pays consiste en un mélange pragmatique de coopération et de concurrence nécessaires, y compris dans le domaine de l'intelligence artificielle. Leurs relations sont amenées à devenir de plus en plus marquées par la concurrence économique et technologique et par un risque de l'affrontements. À l'avenir, l'intelligence artificielle sera un facteur déterminant de l'équilibre des pouvoirs.

¹⁸⁶ Armbruster A. (2020, 7 septembre) Wer in der KI führt, dominiert wirtschaftlich und militärisch ; Frankfurter Allgemeine.

<https://www.faz.net/aktuell/wirtschaft/digitec/usa-gegen-china-ki-fachmann-zur-kuenstlichen-intelligenz-16942865.html?GEPC=s9>

¹⁸⁷ Tchakarova V. Is a Cold War 2.0 Inevitable ; Observer Research Foundation.

<https://www.orfonline.org/expert-speak/is-cold-war-2-inevitable/>

¹⁸⁸ Malhotra R. (2021) Artificial Intelligence and The Future Of Power : 5 Battlegrounds ; Rupa.

¹⁸⁹ Tchakarova V. (2021) Le Dragonbear : Axe de commodité ou nouveau mode de structuration du système mondial? ; Irmo Brief.

<https://www.aies.at/publikationen/2020/the-dragon-bear.php> et

Tchakarova V. (2022a) Enter the 'DragonBear' : The Russia-China Partnership and What it Means for Geopolitics, Observer Research Foundation.

<https://www.orfonline.org/research/enter-the-dragonbear/>

Le concept de colonisation numérique introduit par Malhotra¹⁹⁰, de plus en plus pertinent met en évidence la lutte entre le modèle de gouvernance autoritaire doté d'un marché de données fermé, et celui de la gouvernance libérale pourvu d'un marché de données ouvert. Les tensions politiques, idéologiques et économiques entre ces différents types d'acteurs façonnent la géopolitique de la technologie.

Considérées comme les plus grandes démocraties numériques du monde, l'Europe et l'Inde ont pris position contre le comportement des grandes entreprises technologiques chinoises souvent soumises à des restrictions voire interdites. L'IA devenant un élément clé de la course mondiale à la suprématie technologique, les choix stratégiques et les alliances de l'Europe et de l'Inde joueront un rôle déterminant dans l'issue de la bataille pour la domination numérique.

*The Guardian*¹⁹¹ a nommé les données le pétrole du XXI^e siècle. Dans ce contexte, l'IA apparaît comme un catalyseur important dans la géopolitique de la technologie¹⁹². Pour s'opposer à la colonisation numérique chinoise, les États-Unis et l'Inde sont susceptibles de coopérer et de coordonner leurs actions et leurs mesures. Malgré la crainte de déclencher une « nouvelle guerre froide » à la lumière des tensions actuelles entre la Russie et l'Ukraine et des manœuvres militaires croissantes de la Chine dans le détroit de Taïwan, le président Biden a soutenu les initiatives de son prédécesseur visant à isoler la Chine des réseaux commerciaux et technologiques mondiaux. En 2022, les États-Unis ont adopté la loi CHIPS pour accroître la production nationale de semi-conducteurs, renforcer la sécurité économique et nationale et affaiblir la Chine¹⁹³. Cette loi entend décourager les bénéficiaires de subvention de développer la fabrication de semi-conducteurs en Chine pendant une période de dix ans à compter de la date d'attribution de la subvention. Le Bureau de l'industrie et de la sécurité (BIS) du Ministère américain du commerce a de plus imposé des restrictions à l'exportation visant le développement par la Chine des technologies essentielles, en particulier de semi-conducteurs. Ces mesures illustrent la crainte de l'administration Biden que les puces et équipements avancés ne facilitent le développement de nouvelles armes par la Chine et ne renforcent son réseau de surveillance numérique.

Dans ce contexte, la coopération bilatérale russo-chinoise dans le domaine de l'IA, composante d'un vaste partenariat stratégique entre les présidents des deux pays, n'a cessé de s'intensifier malgré les

¹⁹⁰ Chaudhuri R. (2020, 4 décembre) India and the geopolitics of technology ; The Hindustan Times.

<https://www.hindustantimes.com/analysis/india-and-the-geopolitics-of-technology/story-dd2DGyVvuhH7XmOfVSpLwL.html>

¹⁹¹ Arthur, Charles. (2013, 23 août). Tech Giants may be Huge, But Nothing Matches Big Data ; The Guardian.

<https://www.theguardian.com/technology/2013/aug/23/tech-giants-data>

¹⁹² Raibagi K. (2020, 10 novembre) ; The Role Of AI Collaboration In India's Geopolitics ; Analytics India Magazine.

<https://analyticsindiamag.com/the-role-of-ai-collaboration-in-indias-geopolitics/>

¹⁹³ Calabrese J. (2022) CHIPS on the table : Escalating US-China tech war impacts the Mideast ; The Middle East Institute. <https://www.mei.edu/publications/chips-table-escalating-us-china-tech-war-impacts-mideast>

tentatives des États-Unis et de l'Europe de l'entraver par diverses sanctions. Samuel Bendett, qui travaille au *Center for Naval Analyses*, considère qu'une grande part de la coopération entre Moscou et Pékin se déroule en dehors du secteur de la Défense. Dans le même temps, le développement des liens militaires entre les deux pays offre de nouvelles opportunités d'établir une coopération plus globale et il existe des preuves de l'approfondissement des contacts bilatéraux dans la sphère militaire. Citant un exemple de confiance accrue entre les deux pays, M. Bendett souligne l'aide apportée par la Russie à la Chine pour la création d'un système d'alerte précoce pour les tirs de missiles.

Les conséquences du renforcement de cette relation pour la stratégie américaine et les relations entre les États-Unis et la Russie, deviendront de plus en plus importantes. L'élan avec lequel la Russie et la Chine construisent de nouveaux systèmes d'intelligence artificielle alarme certains dirigeants et experts américains qui voient à travers ce dernier transparaître la volonté russo-chinoise de remettre en question l'avantage technique acquis par l'armée américaine.

Ces deux pays participent activement à la course à l'IA et pourraient collectivement dépasser le Pentagone si ce dernier ne décide pas d'agir de manière décisive. Néanmoins, la coopération entre la Russie et la Chine dans le domaine n'en est qu'à ses débuts. En effet, de nombreux programmes ont débuté il y a moins de cinq ans. Pour autant, Edmonds note que la Russie et la Chine ont déjà dépassé les États-Unis en termes d'ampleur de leur collaboration. Dans un contexte de tensions croissantes avec les États-Unis, la Chine et la Russie ont clairement convenu d'étendre leur partenariat technique, et l'IA joue un rôle clé dans leurs plans pour l'avenir¹⁹⁴.

En conclusion, la coopération scientifique et technologique est devenue un pilier important du « partenariat stratégique global » entre la Chine et la Russie. L'IA est l'une des technologies clés auxquelles la coopération technologique sino-russe accorde une grande priorité. Comme indiqué dans l'étude de cas sur la surveillance de masse pendant la période de Covid-19, la Russie a suivi l'exemple de la Chine et mis en place un système de vidéosurveillance à grande échelle comprenant la reconnaissance faciale.

Sur la base de cette analyse, le dernier chapitre de ce rapport présente trois scénarii - mutuellement non exclusifs - pour le développement à venir de la coopération technologique sino-russe et le déploiement de la technologie de surveillance numérique en Russie à la lumière de la guerre en Ukraine. Enfin, le rapport propose des recommandations sur la manière dont la France et l'UE peuvent répondre à ces scénarios.

6.1 Scénario 1 - La coopération technologique entre la Russie et la Chine s'intensifie en raison de la guerre en Ukraine

Le premier scénario concerne la trajectoire de la coopération technologique entre la Russie et la Chine. On peut s'attendre à ce que, compte tenu de la guerre en Ukraine, la coopération technologique sino-russe s'intensifie, tant au niveau politique qu'industriel. Lors de sa visite à Moscou en mars 2023, Xi Jinping a signé avec Vladimir Poutine un nouvel accord bilatéral sur la

¹⁹⁴ Lisez l'article complet sur ce lien : https://www.actualno.com/analysis/newsweek-rusija-syzdava-armija-ot-roboti-a-kitaj-j-pomaga-s-izkustven-intelekt-news_1599211.html

coopération dans le domaine des technologies de l'information et de l'économie numérique. Selon Soldatov et Borogan¹⁹⁵, dans cet accord, la partie russe a fait des concessions importantes, bien que non déclarées. Les universités russes sont désormais, i.e. depuis l'invasion de l'Ukraine, plus ouvertes aux étudiants et chercheurs chinois. C'est notamment le cas de l'université technique Bauman de Moscou, plus grande école d'ingénieurs de Russie, qui en juillet 2022 a accepté de s'associer à l'université russo-chinoise de Shenzhen (suite à une initiative lancée conjointement par l'Institut technologique de Pékin et l'Université d'État de Moscou).

Au niveau des entreprises, les importations russes de machines et de composants électriques ainsi que d'autres produits à double usage ont augmenté depuis l'invasion de l'Ukraine. Selon les données collectées par le « *Russian foreign trade tracker* » de Bruegel, la Russie a en 2022 importé pour 4,5 milliards d'euros (4,8 milliards de dollars) de machines et de composants électroniques de Chine, contre 4,3 milliards d'euros (4,6 milliards de dollars) en 2021¹⁹⁶. Les données montrent que ces importations ont chuté à partir de janvier 2022, pour ensuite reprendre fortement à partir de juin 2022¹⁹⁷. Cette augmentation est concomitante à la réduction des exportations de produits chinois vers la Russie par les grandes entreprises technologiques chinoises comme Huawei, qui craignaient les sanctions américaines¹⁹⁸. Ce rebond à l'export est donc le fait d'entreprises chinoises moins connues et moins exposées sur les marchés internationaux¹⁹⁹. Par ailleurs, les produits chinois exportés vers la Russie comme les semi-conducteurs, transitent souvent par des pays tiers comme la Turquie ou les Émirats arabes unis, ce qui permet à la Chine de réduire le risque de faire l'objet de sanctions²⁰⁰. Malgré ces évolutions, le partage de technologies IA innovantes à vocation militaire restera probablement une ligne rouge pour la Russie dans le cadre de sa coopération technologique avec la Chine.

6.2 Scénario 2 - La Russie deviendra de plus en plus dépendante de la technologie chinoise

Dans le même temps, le renforcement de la coopération technologique entraîne également une dépendance croissante de la Russie à l'égard de la technologie chinoise. L'indépendance technologique accrue de la Russie pourrait perturber le paysage technologique et géopolitique mondial si les tendances actuelles se poursuivent.

Bloomberg a récemment mentionné un mémorandum rédigé à l'été 2022 par des fonctionnaires du Ministère russe du développement numérique, des communications et des médias. Dans ce dernier, les élites russes font part de leurs inquiétudes quant à la dépendance croissante de leur pays à l'égard de la technologie chinoise, en particulier des processeurs, des équipements de réseaux et plus généralement de tous les composants électroniques. Les auteurs craignent que la dépendance des réseaux de communication aux solutions chinoises comme celles fournies par Huawei, constitue un

¹⁹⁵ Soldatov & Borogan, 2023

¹⁹⁶ Darvas et al, 2023

¹⁹⁷ Darvas et al, 2023

¹⁹⁸ Seddon & Leahy, 2023

¹⁹⁹ Seddon & Leahy, 2023

²⁰⁰ Seddon & Leahy, 2023

danger pour la sécurité des données et la fiabilité des réseaux. Par ailleurs, ils suggèrent que la dépendance à la Chine puisse entraîner une réduction du dynamisme industriel en Russie²⁰¹.

Le mémorandum propose une liste de contre-mesures destinées à la fois à atténuer la dépendance de la Russie à l'égard de la technologie chinoise, et à promouvoir la production nationale d'équipements critiques (e.g. imposer des quotas sur les produits chinois, pousser les entreprises chinoises à transférer leur production en Russie, exiger des fournisseurs chinois qu'ils utilisent des ressortissants et des sous-traitants russes, limiter l'utilisation d'équipements sans marque, et offrir des incitations telles que des contrats à long terme et des subventions aux développeurs et aux entreprises de télécommunication russes)²⁰². Il convient cependant de noter que, par le passé, les tentatives de l'armée russe de remplacer dans ses systèmes d'armement les composants étrangers par des pièces produites localement ont échoué. Compte tenu des circonstances actuelles, il est difficile d'imaginer que de telles initiatives soient couronnées de succès. En effet, les États-Unis et l'Union européenne redoublant d'efforts pour réduire les moyens permettant à la Russie de contourner les sanctions, celle-ci pourrait à l'avenir avoir plus de mal à importer des composants informatiques et électroniques américains et européens. Ce qui réduirait à néant sa capacité à disposer d'un levier sur la Chine. Il est donc probable que la dépendance russe à l'égard des technologies chinoises ne fasse que s'accroître, reléguant la Russie au rang de « partenaire junior » de la Chine.

6.3 Scénario 3 - L'autoritarisme numérique se développera en Russie

Le troisième scénario concerne l'utilisation d'outils numériques pour la surveillance de masse en Russie. Comme indiqué dans l'étude de cas du chapitre 5, la pandémie de Covid-19 a permis aux autorités russes de tester et d'étendre leur système de contrôle numérique. Les autorités russes ont appris à travailler avec des outils numériques tels que les QR codes et a repéré les violations de la quarantaine par le biais de caméras de surveillance et d'applications téléphoniques²⁰³. Enfin, les systèmes de vidéosurveillance dotés de capacités de reconnaissance faciale ont été étendus à tout le pays. Ces systèmes de vidéosurveillance sont restés en place après la pandémie et, depuis l'invasion de l'Ukraine, ont été utilisés non seulement pour arrêter et détenir des manifestants antigouvernementaux, parfois même à titre préventif, mais aussi pour convoquer massivement les citoyens par le biais du portail électronique des services gouvernementaux (qui ne nécessite ni l'application du portail, ni même la possession d'un téléphone).

Il est donc probable que la Russie prenne de nouvelles mesures autoritaires. Si avant l'annonce de la mobilisation partielle, l'utilisation la plus menaçante de la surveillance numérique était l'identification de la population mobilisable, en 2023, l'Etat est passé à la prochaine étape soit à l'utilisation de la surveillance pour mobiliser les citoyens, un scénario élaboré par Soldatov, qui parle d'un « GULAG » économique et numérique. Étant donné que les élites russes considèrent la Chine comme un modèle d'utilisation des outils numériques pour la surveillance et le contrôle de masse, les autorités russes pourraient également mettre en place un système de contrôle numérique comparable au système de crédit social chinois.

²⁰¹ Nardelli, 2023

²⁰² Nardelli, 2023

²⁰³ Stanovaya, 2023

Ces trois scénarios constituent des orientations plausibles pour les relations sino-russes en matière d'IA. Le premier, soit « la coopération technologique sino-russe s'intensifie en raison de la guerre en Ukraine » semble le plus probable. Plusieurs facteurs le suggèrent.

Premièrement, l'accord bilatéral signé lors de la visite d'État de Xi Jinping à Moscou en mars 2023 témoigne d'un engagement formel à renforcer la coopération technologique, y compris dans le domaine de l'IA. Deuxièmement, les universités russes se sont ouvertes aux étudiants et aux chercheurs chinois, signe d'une collaboration accrue dans le domaine de la technologie et de la recherche. Troisièmement, malgré les sanctions et la baisse initiale des importations, les importations russes de machines et de composants électroniques en provenance de Chine ont augmenté, ce qui témoigne d'un alignement pratique de leurs secteurs technologiques. Les entreprises chinoises moins connues qui complètent les géants de la technologie comme Huawei sont la preuve d'une forme de résilience de la coopération technologique sino-russe.

Toutefois, il est important de noter que ce scénario n'exclut pas les deux autres. Le renforcement de la coopération technologique avec la Chine (scénario 1) peut entraîner une dépendance accrue de la Russie à l'égard de la technologie chinoise (scénario 2) et contribuer à la montée de l'autoritarisme numérique en Russie (scénario 3). Ces scénarios peuvent se dérouler simultanément ou séquentiellement. Il est également possible que de nouveaux facteurs non pris en compte dans ces scénarii apparaissent et influencent la trajectoire de la coopération sino-russe en matière d'IA.

Plusieurs scénarii commencent à émerger dans le paysage sécuritaire mondiale. Tout d'abord l'adoption généralisée de l'IA dans le contrôle de la qualité au sein des diverses industries de défense, y compris pour du contrôle qualité non destructif, c'est-à-dire qui utilise l'IA pour inspecter les produits semi-finis et les unités d'assemblage.

Deuxièmement, la nature de la dynamique des conflits pourrait être considérablement modifiée. L'intégration croissante de l'IA dans les stratégies militaires devrait révolutionner la guerre. La prise de décision pourrait être facilitée par la capacité de l'IA à analyser rapidement et avec précision de grandes quantités de données.

Troisièmement, l'intégration active et continue de l'IA dans les stratégies militaires de pays comme la Chine et la Russie marque l'avènement d'une nouvelle course aux armements dotés d'IA. Cette concurrence mondiale potentielle modifiera considérablement les équilibres de pouvoir et nécessitera de mettre davantage l'accent sur les capacités de défense liées à l'IA. L'impératif de rester compétitif a poussé les nations à accélérer la recherche, le développement et la mise en œuvre de l'IA dans les applications militaires.

Enfin, un recours accru dans les opérations militaires aux technologies produites par des groupes privés pourrait également se manifester. La tendance à l'adoption généralisée de ces technologies, observée dans la guerre russe contre l'Ukraine, pourrait induire un changement stratégique dans les guerres futures. Comme les technologies disponibles continueront d'évoluer, les armées du monde entier pourraient devoir s'adapter et intégrer ces avancées dans le champ opérationnel.

6.4 Recommandations

Sur la base des scénarii décrits ci-dessus, les recommandations suivantes peuvent être résumées à l'intention de l'Union européenne et de la France :

1. La France et l'UE devraient revoir et améliorer les sanctions sur l'exportation de composants informatiques et électroniques à double usage, tels que les processeurs, les équipements de réseau et plus généralement les semi-conducteurs, à destination de la Russie. Des efforts sont particulièrement nécessaires pour s'assurer que les sanctions ne sont pas contournées par des intermédiaires situés dans des pays tels que la Turquie, la Chine (y compris Hong Kong) ou les Émirats arabes unis. Les technologies occidentales à double usage jouent non seulement un rôle essentiel dans les systèmes d'armement russes, mais les composants électroniques produits aux États-Unis ou en Europe sont également nécessaires au développement de logiciels de reconnaissance faciale utilisés par les autorités russes dans le cadre de la lutte contre les opposants politiques. Le système de traçabilité des produits tout au long de la chaîne de valeur, de mise en œuvre effective des sanctions et des pénalités devrait être révisé et mis à jour. Bien qu'il nécessite un investissement important, le coût associé pourrait être partagé avec les acteurs privés, en premier lieu les producteurs d'équipements. Dans ce contexte, le renforcement du régime de sanctions augmentera probablement encore la dépendance de la Russie à l'égard des fournisseurs chinois.

2. Améliorer la traçabilité des chaînes de valeur et la mise en œuvre des sanctions : il est essentiel d'améliorer le système de traçage des chaînes de valeur des produits et de mise en œuvre des sanctions. Cela implique de mettre au point des mécanismes solides pour suivre de bout en bout le parcours des technologies à double usage. La collaboration avec les acteurs privés, y compris les producteurs d'équipements, est cruciale à cet égard.

3. Engager des dialogues et des coopérations en matière de cyber sécurité : compte tenu de la prolifération des systèmes de surveillance et de contrôle numériques, l'Union européenne et la France devraient s'engager activement dans des dialogues internationaux sur les normes et les réglementations relatives à la surveillance numérique, à l'IA et à la cyber sécurité.

4. Créer des centres nationaux et européens d'intelligence artificielle pour observer et évaluer les activités de la Chine, de la Russie et des autres compétiteurs. Suivre les progrès de la Russie et de la Chine en matière de technologies autonomes et robotiques, y compris l'utilisation des drones dans la stratégie militaire et la transformation potentielle des technologies commerciales telles que les drones DJI Mavic dans les scénarios de conflit. Voici quelques exemples de coopération entre la Chine et la Russie qu'il convient de surveiller de près et qui peuvent contribuer à l'élaboration de futures sanctions à l'encontre de la Russie :

- a) Création de centres de recherche conjoints : L'Institut de physique et de technologie de Moscou (MIPT) et Huawei ont mis en place un centre de recherche conjoint sur l'IA. Ce centre se concentre sur l'apprentissage profond, les algorithmes de prise de décision, la vision par ordinateur et d'autres avancées liées à l'IA.
- b) Collaboration universitaire sino-russe : L'Institut de technologie de Pékin et l'Université d'État de Moscou ont créé une université russo-chinoise à Shenzhen en 2014. Cette entité commune se concentre sur l'échange d'étudiants et de chercheurs et encourage la coopération et les progrès dans des domaines tels que l'IA.

- c) *Projet chinois des nouvelles routes de la soie (BRI)* : la Russie soutient le projet chinois de la BRI, qui est un plan ambitieux visant à relier l'Asie à l'Afrique et à l'Europe par le biais de réseaux terrestres et maritimes. L'initiative comporte des aspects technologiques importants, notamment l'amélioration de l'infrastructure numérique et de la technologie de l'IA dans les pays participants.
- d) *Alliance IA contre COVID-19* : La Russie et la Chine utilisent l'IA pour lutter contre le COVID-19. Elles partagent leurs données et leurs ressources en matière d'IA afin de développer de meilleurs modèles prédictifs, d'améliorer le diagnostic et de soutenir le développement de vaccins.
- e) *Exercices militaires conjoints* : La Russie et la Chine ont mené des exercices militaires conjoints, tels que l'opération « Vostok ». Ces exercices font appel à des technologies sophistiquées, notamment des systèmes autonomes, ce qui témoigne d'une coopération dans le domaine militaire également.

Si ces exemples témoignent d'une coopération entre les deux pays, ils n'impliquent pas nécessairement le partage d'innovations sensibles en matière d'IA, en particulier dans le domaine militaire, car les deux pays restent prudents quand il s'agit de partager les résultats de leurs recherches et développements avancés en matière d'IA.

Conclusion :

Alors que la Chine progresse vers l'autonomie technologique, elle cherche toujours à s'intégrer dans l'espace scientifique et technologique mondial et à s'engager dans la coopération internationale. Si la Chine apprécie les contributions de la Russie dans le domaine de la science fondamentale, la Russie a, elle, beaucoup à apprendre de la réussite de la Chine en matière de commercialisation des résultats de R&D. La Russie et la Chine ont des appréhensions différentes de la souveraineté technologique. La Russie et la Chine ont également des conceptions différentes de la souveraineté technologique. Pour la Chine, il s'agit d'être en mesure de produire des produits essentiels, de maîtriser les technologies de base et d'être compétitif au niveau mondial. À l'inverse, pour la Russie, il s'agit d'acquérir des technologies fondamentales qui lui permettent de rivaliser avec l'Occident et d'éviter d'être à la traîne en matière de développement.

Le pays qui sortira vainqueur de la quatrième révolution industrielle en cours n'est pas encore connu. Néanmoins, le vainqueur affirmera certainement sa domination sur ses concurrents et ses alliés en établissant de nouvelles normes et règles dans les affaires mondiales. Logiquement, il ne peut y avoir qu'un seul vainqueur dans une compétition aussi décisive. Pour tenter de dominer la quatrième révolution industrielle, il faudra rechercher une plus grande autosuffisance en matière d'intelligence artificielle (IA), de technologies essentielles et de chaînes mondiales d'approvisionnement. Il ne fait aucun doute que la bataille pour la domination mondiale se jouera entre les États-Unis et la Chine, mais le rôle de la Russie, de l'UE et de l'Inde sera déterminant pour le résultat final.

Bibliographie

1. Balding, C. & Clarke, D.C. (2019). *Qui est propriétaire de Huawei ?* (article de SSRN). Consulté à l'[adresse](http://dx.doi.org/10.2139/ssrn.3372669) : <http://dx.doi.org/10.2139/ssrn.3372669>.
2. Barros, G. (2020). La Russie en revue : Poutine déploie de nouveaux contrôles autoritaires pendant la pandémie de Covid-19. *Institut pour l'étude de la guerre*. Consulté sur : <https://www.understandingwar.org/backgrounder/russia-review-putin-deploys-new-authoritarian-controls-during-covid-19-pandemic>.
3. Bendett, S. & Kania, E.B. (2019). Un nouveau partenariat sino-russe de haute technologie : L'innovation autoritaire à l'ère de la rivalité des grandes puissances. *Institut australien de politique stratégique (ASPI) Policy brief Report No. 22/2019*. Consulté à l'[adresse suivante](https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership) : <https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership>.
4. Borak, M. (2023, 6 février). Inside Safe City, Moscow's AI Surveillance Dystopia (À l'intérieur de Safe City, la dystopie de surveillance de l'IA de Moscou). *Wired*. Tiré de : <https://www.wired.com/story/moscow-safe-city-ntechlab/>.
5. Brewster, T. (2020, 22 septembre). Cette start-up russe spécialisée dans la reconnaissance faciale prévoit de mondialiser sa technologie de « détection des agressions » grâce à un financement de 15 millions de dollars provenant de fonds souverains. *Forbes*. Consulté sur : <https://www.forbes.com/sites/thomasbrewster/2020/09/22/this-russian-facial-recognition-startup-plans-to-take-its-aggression-detection-tech-global-with-15-million-backing-from-sovereign-wealth-funds/#23045ef54b9e>.
6. Darvas, Z., Martins, C. et McCaffrey, C. (2023, 25 avril). Suivi du commerce extérieur russe [Dataset]. Bruegel. Tiré de : <https://www.bruegel.org/dataset/russian-foreign-trade-tracker>.
8. Deng, I. (2022, 20 décembre). Huawei disbands enterprise business team in Russia in further pullback amid Western sanctions, local media reports. *South China Morning Post*. Consulté à l'[adresse](https://www.scmp.com/tech/big-tech/article/3203995/huawei-disbands-enterprise-business-team-russia-further-pullback-amid-western-sanctions-local-media?module=perpetual_scroll_0&pgtype=article&campaign=3203995) : https://www.scmp.com/tech/big-tech/article/3203995/huawei-disbands-enterprise-business-team-russia-further-pullback-amid-western-sanctions-local-media?module=perpetual_scroll_0&pgtype=article&campaign=3203995.
9. Edmonds, J., Bendett, S., Fink, A., Chesnut, M., Gorenburg, D., Kofman, M., Stricklin, K. et Waller, J. (2021). *Intelligence artificielle et autonomie en Russie*. Arlington, VA : Center for Naval Analyses. Tiré de : <https://www.cna.org/our-media/newsletters/ai-and-autonomy-in-russia>.
10. Rapport de l'AIIC (2022) : <https://www.cna.org/reports/2022/09/Artificial-Intelligence-and-Autonomy-in-Russia-A-Years-Reflection.pdf>.
11. Faulconbridge, G. (2023, 16 janvier). Russia produces first set of Poseidon super torpedoes - TASS. *Reuters*. Tiré de : <https://www.reuters.com/world/europe/russia-produces-first-nuclear-warheads-poseidon-super-torpedo-tass-2023-01-16/>.
12. Factiva. (2023). Factiva Company Report : Zhejiang Dahua Technology Co. Ltd. Extrait de : <https://global.factiva.com/ar/arpdf.aspx?pp=PDF>.
13. Fedasiuk, R. (2020). Perspectives chinoises sur l'IA et les capacités militaires futures. *CSET Policy Brief*. Tiré de : <https://cset.georgetown.edu/publication/chinese-perspectives-on-ai-and-future-military-capabilities/>.
14. "Le gouvernement acquiert des actions de la Sberbank auprès de la Banque centrale pour 29 milliards de dollars. (2020, 20 avril). *Agence de presse russe TASS*. Tiré de : <https://tass.com/economy/1142851>.

15. Huawei. (2022). *Huawei Investment & Holding Co, Ltd. 2021 Annual Report*. Extrait de : <https://www.huawei.com/en/annual-report/2021>.
16. Hynek, N. et Solovyeva, A. (2022). *Chapitre 3 : Militarisation de l'intelligence artificielle aux États-Unis, en Russie et en Chine*. In : *Militarisation de l'intelligence artificielle : Theory, Technology, and Regulation*, p. 49-84. New York : Routledge.
17. Ilyushina, M. (2020, 14 avril). Moscou met en place un système de suivi numérique pour renforcer le confinement. Les critiques parlent d'un « cyber-goulag ». *CNN*. Tiré de : <https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html>.
18. Kania, E.B. (2017). *La singularité du champ de bataille : Artificial Intelligence, Military Revolution, and China's Future Military Power (Intelligence artificielle, révolution militaire et puissance militaire future de la Chine)*. Washington D.C. : Centre pour une nouvelle sécurité américaine. Consulté à l'adresse suivante : <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>.
19. Kania, E.B. (2019). L'innovation militaire chinoise dans la révolution de l'IA. *The RUSI Journal*, 164(5-6), 26-34. Retrieved from: <https://doi.org/10.1080/03071847.2019.1693803>.
20. Khalil, L. (2020, 2 novembre). *L'autoritarisme numérique, la Chine et le COVID*. Sidney : Lowy Institute. Tiré de : <https://www.lowyinstitute.org/publications/digital-authoritarianism-china-covid>.
21. Larsen, B.C. (2019). L'équipe nationale d'IA de la Chine : Le rôle des plateformes nationales d'innovation ouverte en matière d'IA. Dans G. Webster (Ed.), *AI Policy and China : Realities of State-Led Development* (Stanford-New America Digichina Project Special Report No. 1) (p. 16-20). Tiré de : <https://d1y8sb8igg2f8e.cloudfront.net/documents/DigiChina-AI-report-20191029.pdf>.
22. Li, T. (2019, 29 avril). Qui contrôle Huawei ? La structure de l'actionnariat du leader chinois des télécoms expliquée plus en détail. *South China Morning Post*. Consulté à l'adresse : <https://www.scmp.com/tech/tech-leaders-and-founders/article/3007863/who-controls-huawei-chinese-telecom-leaders>.
23. Lo, K. (2022). COVID-19 et la montée de l'État de surveillance en Chine. *Melbourne Asia Review*, 11. Consulté à l'adresse : <https://dx.doi.org/10.37839/MAR2652-550X11.5>
24. Markotkin, N. (2021). Le coronavirus annonce-t-il l'ère de la surveillance totalitaire en Russie et en Eurasie ? *Carnegie Endowment for International Peace*. Tiré de : <https://carnegiemoscow.org/commentary/84044>.
25. Masri, L. (2023, 28 mars). La reconnaissance faciale aide Poutine à juguler la dissidence avec l'aide de la technologie américaine. *Reuters*. Tiré de : https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/?utm_source=Sailthru&utm_medium=Newsletter&utm_campaign=Weekend-Briefing&utm_term=041523.
26. Morgan, F.E., Boudreaux, B., Lohn, A.J., Ashby, M., Curriden, C., Klima, K. et Grossman, D. (2020). *Applications militaires de l'intelligence artificielle : Ethical Concerns in an Uncertain World (Applications militaires de l'intelligence artificielle : préoccupations éthiques dans un monde incertain)*. Santa Monica, CA : RAND Corporation. Consulté à l'adresse : https://www.rand.org/pubs/research_reports/RR3139-1.html.
27. Munzinger-Archiv. (2022). Eintrag » Gref, German". In *Munzinger Online/Personen - Internationale Biographisches Archiv*. Tiré de : <https://www.munzinger.de/search/portrait/German+Gref/0/24915.html> [Traduction propre].

28. Nardelli, A. (2023, 19 avril). Russian Memo Said War Leaves Moscow Too Reliant on Chinese Tech. *Bloomberg*. Tiré de : https://www.bloomberg.com/news/articles/2023-04-19/russia-china-worries-set-out-in-private-memo-on-tech-risk?cmpid=BBD041923_OEU&utm_medium=share&utm_source=website&utm_term=230419&utm_campaign=mobile_web_share.
29. Nocetti, J. (2020). Un outsider paradoxal : La Russie dans la course à l'intelligence artificielle. *Russie.Nei.Reports*, No. 34. Paris : Institut français des relations internationales (IFRI). Récupéré de : https://www.ifri.org/sites/default/files/atoms/files/nocetti_russie_intelligence_artificielle_2020.pdf.
30. Rostec. (2018, 26 mars). Rostec va investir dans la technologie de reconnaissance faciale [Communiqué de presse]. Tiré de : <https://rostec.ru/en/news/rostec-to-invest-in-face-recognition-technology/>.
31. "Un milliardaire russe investit dans la technologie de reconnaissance faciale. (2017, 12 mai). *East-West Digital News*. Consulté à l'adresse : <https://www.ewdn.com/2017/05/12/russian-billionaire-invests-in-face-recognition-technology/>.
32. Sberbank. (n.d.). SberBank history [Website]. Tiré de : <https://www.sberbank.com/about/history>.
33. Sberbank. (2020, 1er décembre). Sber présente la stratégie de développement 2023 [Communiqué de presse]. Tiré de : <https://www.publicnow.com/view/5BE04BA4EE76EAFFAE93969CBA44EB80A696CD68>.
34. Seddon, M. et Leahy, J. (2023, 21 mars). Les entretiens entre Xi Jinping et Vladimir Poutine soulignent le rôle de la Russie en tant que « partenaire junior » de la Chine. *Financial Times*. Consulté sur : <https://www.ft.com/content/73d50de6-53c8-4bf6-adf9-8cf108f82ca1>.
35. Simes, D. (2020, 4 février). Huawei joue un rôle de premier plan dans le nouveau partenariat Chine-Russie en matière d'IA. *Nikkei Asia*. Tiré de : <https://asia.nikkei.com/Spotlight/Asia-Insight/Huawei-plays-star-role-in-new-China-Russia-AI-partnership>.
36. Soldatov, A. et Borogan, I. (2023, 23 mars). China Finally Enters the Russia's Technological Treasure House (La Chine entre enfin dans la maison des trésors technologiques de la Russie). *Centre d'analyse des politiques européennes (CEPA)*. Tiré de : <https://cepa.org/article/china-finally-enters-russias-technological-treasure-house/>.
37. Stanovaya, T. (2023, 17 avril). La nouvelle loi russe sur la conscription rapproche considérablement le goulag numérique. *Carnegie Politika*. Consulté à l'adresse : <https://carnegieendowment.org/politika/89553>.
38. "'State Services R Us' - La construction d'un 'goulag numérique' pour les Russes qui ne peuvent être appelés sous les drapeaux se transforme en un véritable casse-tête pour l'entrepreneur en informatique du gouvernement". (2023, 25 avril). *Meduza*. Tiré de : <https://meduza.io/en/feature/2023/04/25/state-services-r-us>.
39. Stecklow, S., Gauthier-Villars, D. et Tamman, M. (2022, 13 décembre). La chaîne d'approvisionnement qui maintient la technologie en Russie. *Reuters*. Tiré de : <https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-tech-middlemen/>.
40. Vardanyan, Broitman and Partners. (n.d.). About the Company [Website]. Extrait de : <https://vbpartners.ru/en/about-the-company.html>.

41. « Celui qui sera à la tête de l'IA dominera le monde » : Poutine aux enfants russes à l'occasion de la journée du savoir". (2017, 1er septembre). *RT International*. Consulté à l'adresse : <https://www.rt.com/news/401731-ai-rule-world-putin/>.
42. Xu, F. et Liu, Q. (2021). China : Community Policing, High-Tech Surveillance, and Authoritarian Durability. Dans V.V. Ramraj (ed.), *Covid-19 in Asia : Law and Policy Contexts* (p. 27-C2.N100). Oxford : Oxford University Press. Retrieved from: <https://doi.org/10.1093/oso/9780197553831.003.0002>.
43. [Xu Xu](#), [Genia Kostka](#), and [Xun Cao](#), "Information Control and Public Support for Social Credit Systems in China," *The Journal of Politics*, 84:4, October 2022, <https://www.journals.uchicago.edu/doi/full/10.1086/718358>.



Russian-Chinese alliance in artificial intelligence, and how it has evolved since the invasion of Ukraine

Author: Sebastian Linke

Editor: Velina Tchakarova

11/09/2023

Introduction

As a result of Russia's invasion of Ukraine, a new dynamic of alliance between Russia and China has manifested itself that could upset the balance of power in the Eurasian area and beyond.

In an attempt to limit its growing isolation on the international stage in the face of Western sanctions, Russia has increasingly turned to China as an economic, financial, technology and military partner since 2014. Beijing in turn seeks to preserve an ambiguous posture as to its support of the war, which consists of reasserting its strategic autonomy and preserve its business and diplomatic ties with the West, while taking advantage of Russia's economic isolation and using it as a means to increase its own geopolitical influence.

This report analyses the evolution of the Russian-Chinese alliance in the fields of artificial intelligence, how these two parallel partnerships are evolving, and what they mean for the future of global governance. It focuses on the geopolitical, commercial and geo-economic forces that underlie the relationship between Moscow and Beijing, and how the war in Ukraine has reshaped the partnership.

The report is a deep-dives into Russia-China relationship in the field of artificial intelligence (AI). It begins with the characteristics and applications of AI, compares Chinese and Russian strategic thinking in the field, and proceeds to explain the ecosystem of key companies working on the technology in both countries, and their relationships with their respective states. Part 2 continues with an analysis of the evolution of Russian-Chinese cooperation in AI and outlines its limitations. It concludes with a joint case study of the use of AI in both countries during COVID for mass surveillance and analysis of the lessons learned by Russia for the subsequent application of AI for the suppression of opposition and mobilization for war ("digital GOULAG"), and with recommendations.

1. Characteristics and applications of Artificial Intelligence

The United Nations Institute for Disarmament Research (UNIDIR) provides a broad definition of Artificial Intelligence (AI) as the “field of study devoted to making machines intelligent”.¹ However, as the standard for machines to be considered ‘intelligent’ is constantly moving, it may be most useful to think of a spectrum of intelligence along which machines can be placed. All existing AI systems fall under the broad category of ‘narrow’ AI, which means that their intelligence is limited to a single task or domain of knowledge.² Meanwhile, researchers consider that it may take many decades until they can develop ‘general’ AI, systems capable of human-level intelligence across a broad range of tasks.³ The prevalent approach to the development of ‘narrow’ AI is machine learning: Learning machines are given a goal to optimize and are meant to derive their own procedures to achieve this goal through the analysis of large training sets utilizing statistical algorithms.⁴ While AI research started in the 1940s, the field experienced a boom in activity around 2010 due to three converging developments which led to the advancement in the state of narrow AI: the increasing availability of large datasets necessary to train AI algorithms, improvements in machine learning, and increases in computing power.⁵

When discussing military applications of AI, one should consider three key characteristics of the technology: Firstly, AI may be integrated across a variety of applications. Secondly, many of these AI applications are dual use, i.e., they have both civil and military applications. Lastly, the integration of AI into a system may not be immediately recognizable as it is a relatively transparent capability. Sayler therefore points out that AI procurement will not result in countable objects, rather algorithms will be integrated into a variety of larger systems.⁶

Accordingly, there is a variety of military applications of AI including intelligence, surveillance and reconnaissance (ISR); logistics, e.g. predictive maintenance; military cyber operations; disinformation operations like ‘deep fakes’; command and control; and autonomous vehicles.⁷ Given the dual use character of AI technologies, Morgan et al. expect that most future military applications will be adaptations of technologies developed in the commercial sector including but not limited to image recognition, text analysis, self-driving cars and game-playing.⁸

¹ UNIDIR, 2018, p. 2

² Ibid, p. 5

³ Sayler, 2020, p. 2

⁴ UNIDIR, 2018, p. 2

⁵ Sayler, 2020, p. 2

⁶ Ibid, p. 3

⁷ Ibid, p. 9-15

⁸ Morgan et al., 2020, p. 13

2. Chinese strategic thinking on Artificial Intelligence

The Chinese government considers AI to be a core aspect of national and military power and prioritizes the development of AI technologies at the highest level. Meanwhile, the Chinese armed forces, the People's Liberation Army (PLA) anticipates that AI could fundamentally change the nature of warfare resulting in a shift to 'intelligent' warfare, in which AI will be as integral as information technology is to today's ways of warfare.⁹ This chapter will first outline China's national strategies and plans on AI development. Then, it will briefly describe the Chinese AI ecosystem. Lastly, it will discuss current and potential military applications of AI pursued by the PLA.

2.1 National strategies and plans

Corresponding to the high priority attributed by the Chinese leadership to AI, several of its national science and technology plans have included a focus on AI development. For example, the 'Made in China 2025' program, which was released in 2015 and should transform China into a leading industrial power, included intelligent manufacturing and robotics as well as a target for the domestic market share of autonomous vehicles. Moreover, the 13th Five-Year National Science and Technology Innovation Plan published in August 2016 prioritized big data as well as intelligent manufacturing and robotics among a series of new megaprojects.¹⁰

The central document underlying China's AI strategy is, however, the New Generation AI Development Plan (henceforth the AI Plan) released in July 2017, which articulates China's ambition to become the "world's primary AI innovation center" by 2030.¹¹ According to the plan, China will advance a three-dimensional agenda in AI: addressing key issues in research and development (R&D), pursuing various products and applications, and building an AI industry worth €141.5 billion (US\$ 150 billion)¹² by 2030.¹³ Meanwhile, the AI Plan also formulates a national strategy of military-civil fusion in the domain of AI as one of the six focus tasks defined by plan is to "strengthen military-civilian integration in the AI domain".¹⁴ For that purpose, the plan calls for the establishment of mechanisms to "normalize communication and coordination among scientific research institutes, universities, enterprises and military industry units" and aims at the development of a new generation of AI technology to support "command and decision-making, military deduction, defense equipment, and other applications."¹⁵

According to Bernhard Seyringer, China's AI development, as per the 'New Generation Artificial Development Plan', is divided into three phases. The initial phase, accomplished in 2020, saw China matching the prowess of other advanced nations in AI. By 2025, China aims to elevate its

⁹ Kania, 2017, p. 4, 12

¹⁰ Kania, 2017, p. 9

¹¹ State Council, 2017, p. 6

¹² Conversion from US-Dollar to Euro is done throughout this paper using an exchange rate of €1 = US\$1.06 (current exchange rate on 26th February 2023)

¹³ Kania, 2017, p. 9

¹⁴ State Council, 2017, p. 21

¹⁵ Ibid



competitiveness across various AI sectors and establish new technological standards by realizing significant advances in foundational research. This could propel China to the global forefront of AI-driven applications. Lastly, by 2030, China aspires to be the world's prime hub for AI innovation.¹⁶

While China has formally declared its ambition to be the global frontrunner in artificial intelligence (AI) within the coming decade, it is critical to acknowledge that Beijing has caught up with (and in some ways might have surpassed) the United States in both commercial and national security applications of AI.¹⁷ The forthcoming technological upheaval, largely driven by AI, is poised to reshape worldwide economic and security networks, akin to the influence of semiconductors, computers, and the Internet over the past twenty-five year.¹⁸ Besides being the cornerstone of digital transformation, AI is anticipated to equip the Chinese Communist Party (CCP) with potent tools to consolidate its authoritarian governance, escalating its capacity for data surveillance, gathering, and interpretation, affecting both domestic and foreign populations and governments.

China is leveraging its access to vast data sets to expedite the development of machine learning algorithms, a pace unmatched by democratic societies due to their concerns over data storage, collection, and security. Moreover, China is amplifying its national, scientific, and military prowess in AI by founding centers of excellence, promoting academic and security programs, and initiating state-funded programs for national, local, and university teams (Seyringer, 2021). Besides making strides in AI, China is also progressing in applications like facial recognition, fintech, armed drones, and 5G networks. Interestingly, in certain areas such as fintech, speech tech or facial recognition, China has outperformed the U.S., primarily due to ethical, moral, constitutional, or normative constraints faced by the latter and other democratic political systems (Allison & Schmidt, 2020).

Books like "AI Superpowers: China, Silicon Valley, and the New World Order" by Dr. Kai-Fu Lee (chairman and CEO, Sinovation Ventures) and "AI and the Future of Power" by Rajiv Malhotra provide an insightful account of China's advancement and objectives in AI. The dynamism, magnitude, and resolution of China's efforts to attain AI supremacy call for diligent examination. The surge in investment, growing pool of scientists and patents in AI technologies, and the upswing in private sector funding are indicative of China's commitment. From fintech and facial recognition to commercial platforms and the Internet of Things, China is paving the way in multiple facets. Additionally, AI-powered drones and 5G networks are giving China an edge globally due to increasing demand from the Middle East and Africa.

Digital technologies, such as AI and data science, are bound to instigate technological innovations in various global domains like public health and climate issues. However, their actual application

¹⁶ Seyringer B. (2021, 10 June); Artificial Intelligence: A Chinese Assassin's Mace; The Defence Horizon.

<https://www.thedefencehorizon.org/post/artificial-intelligence-a-chinese-assassin-s-mace>

¹⁷ Allison G., Schmidt E. (2020) Is China Beating the U.S. to AI Supremacy?; Belfer Center for Science and International Affairs.

<https://www.belfercenter.org/publication/china-beating-us-ai-supremacy>

¹⁸ Ibid

incites numerous ethical, legal, and societal dilemmas¹⁹, which the U.S. and China address differently.

Internally, Chinese leader Xi Jinping and senior officials have called for stricter government oversight of AI as part of work to counter "dangerous storms" facing the country, state media reported. The president and other officials from the ruling Communist Party agreed at a meeting of the National Security Commission to improve security management of network data and AI.

In 2023, Beijing has stepped up a broad campaign to root out perceived national security threats by restricting access to data, conducting raids on foreign consulting firms and strengthening anti-espionage laws. China has also taken steps to tighten state control over AI, with a draft law unveiled recently requiring all AI products to pass a security-standards check before they are put on the market. The draft law states that AI products will have to reflect "core socialist values" and must not "include content for subversion of state power". Beijing also considers "deep fakes" - images and sounds generated by AI that can be stunningly realistic - to pose a "danger to national security and social stability".

The digital transformation could engender surveillance societies, where the state controls all data collection and storage. In this context, China could set a precedent for future authoritarian regimes in the Middle East, Africa, and Asia. Andrew Michta argues: *"We must recognize that we are facing not 'China' as a civilization, but rather a communist power whose ideology has always been at its core totalitarian. What is unfolding before our eyes—and has been underway for three decades since the end of the Cold War—is the second, and possibly decisive and final stage of conflict between liberal democracy and communism,"*²⁰ in other words, between democracy and dictatorship.

2.2 China's AI ecosystem

The Chinese government, and thus by extension, the Chinese Communist Party (CCP), plays a crucial role in the development of the country's AI ecosystem. Between 2005 and 2015, the Chinese government has increased spending on AI by 350% and is now assumed to be very close to spending levels in the United States. All activities, including technology development, are controlled at the highest level by the CCP Central Committee. Moreover, the National Science, Technology and Education Leading Group and the CCP Central Military Commission (CMC) play a key role in policymaking and coordination efforts regarding civilian and military applications of AI respectively.²¹ Moreover, the « National Science and Technology Leading Group », a deliberative

¹⁹ Coeckelbergh C. (2020, 19 May) Corona-App: Ethische, rechtliche und gesellschaftliche Fragen; Der Standard.

<https://www.derstandard.at/story/2000117457544/corona-app-ethische-rechtliche-und-gesellschaftliche-fragen>

²⁰ Michta A.A. (2020, 7 May) The Building Blocks of a China Strategy. The American Interest.

<https://www.the-american-interest.com/2020/05/07/the-building-blocks-of-a-china-strategy/>

²¹ Hynek & Solovyeva, 2022, p. 65



and consultative body of the State Council which was dissolved in 2023, used to play an important role in policy-making and coordination efforts in science and technology matters.²²

Military-relevant research efforts in AI and automation extend across academic institutions, national laboratories, defense industry research institutes, and PLA research institutes. A key role is played by the Chinese Academy of Sciences (CAS) as multiple institutes which are associated with this institution, are involved in research related to AI. This includes the Institute of Intelligent Machines, the Institute of Automation and the National Key Laboratory for Pattern Recognition. Moreover, the Key Laboratory of Intelligent Information Processing of the Institute of Computing Technology is pursuing research on natural language processing and translation and intelligent human-machine interfaces. Moreover, the CAS is participating in various joint research efforts in the domain of AI, in which it partners with other universities as well as private companies. Apart from the CAS, important academic institutions involved in military-relevant research include Tsinghua University, which has established its “Military-Civil Fusion National Defense Peak Technologies Laboratory” in 2017 to pursue dual-advances in AI, as well as Beihang University, which is closely linked to the development of military aeronautical and astronautic technologies, including autonomous unmanned underwater vehicles and intelligent UAVs, including for swarming and manned-unmanned teaming.²³

In 2017, the Chinese Ministry of Science and Technology designated the technology companies Baidu, Alibaba, Tencent and iFlytek as members of an “AI national team”. These companies receive national and local government support, in return they are expected construct so-called “open innovation platforms” in specific technology areas, in which other companies can participate. In 2019, the “AI national team” was expanded to include 15 companies, including Huawei for software and hardware (see Figure 1 below).²⁴ At the same time, China possesses a dynamic start-up ecosystem.²⁵ Chinese AI start-ups have won various international AI competitions indicating that they are on the cutting edge of R&D, including in speech recognition and computer vision.²⁶

²² Hynek & Solvyeva, 2022, p. 65; Wei, C., Hu, T. & Liao, Z. (2023, 7 March). A Guide to China’s 2023 State Council Restructuring. <https://npcobserver.com/2023/03/china-npc-2023-state-council-reorganization/>

²³ Kania, 2017, p. 47-49

²⁴ Larsen, 2019, p. 16-17

²⁵ Kania, 2017, p. 6

²⁶ Kania, 2017, p. 6



Figure 1: Members of China's "AI national team", Source: Larsen, 2019, p. 17

As already mentioned, the PLA wants to leverage the private sector progress in AI development through a national strategy of military-civil fusion while pursuing an expansive R&D agenda itself. China's strategy of military-civil fusion will be directed by the CCP's Military-Civil Fusion Development Commission, which was established in 2017 under the leadership of Xi Jinping himself. Within the PLA, the CMC Science and Technology Commission together with its new CMC Military Scientific Research Guidance Committee will be responsible for the PLA's R&D agenda as well as for military-civil fusion.²⁷ The PLA has also created mechanisms at lower levels to implement military-civil integration including the establishment of the Military-Civil Integration Intelligent Equipment Research Institute, which focuses in particular on robotics, unmanned systems and AI.²⁸ Highlighting the strategic importance attributed to this agenda, the CMC Science and Technology Commission and the Ministry of Science and Technology also jointly issued the 13th Five-Year Science and Technology Military-Civil Fusion Plan in 2017.²⁹

There are also indications that the PLA has started to realize partnerships and mechanisms with the private sector for military-civil fusion in AI: For example, iFlytek, a start-up specialized in intelligent voice recognition and speech-to-text-products, is apparently working with the PLA on a voice recognition and synthesis module and HikVision, a start-up owned by the state-owned China Electronics Technology Group Corporation (CETC), has collaborated with the PLA to utilize its AI-enabled video surveillance technology for national defense and security purposes. Moreover, several new research institutes and joint laboratories have been established which will work on dual-use advances in AI technology.³⁰ For example, a Joint Laboratory for Intelligent Command and Control Technologies was established by the CETC and Baidu.³¹

²⁷ Kania, 2017, p. 12-19

²⁸ Hynek & Solovyeva, 2022, p. 65

²⁹ Kania, 2017, p. 19

³⁰ Kania, 2017, p. 20

³¹ Hynek & Solovyeva, 2022, p. 65

2.3 Military applications of Artificial Intelligence

As already mentioned, the PLA foresees that AI could fundamentally transform the character of warfare. Accordingly, it will likely leverage AI for a range of military applications including autonomous unmanned systems; data fusion, information processing, and intelligence analysis; war-gaming, simulation, and training; defense, offense, and command in information systems (cyber warfare); and intelligent support to command decision-making. Based on the analysis of 58 journal articles written between 2016 and 2020 by PLA officers, defense industry engineers, and academics at leading Chinese universities about AI and future weapons systems, Fediasuk finds that Chinese experts forecast that AI will improve detection, targeting, and strikes against military targets. Moreover, he notes that Chinese experts believe that AI may lower the costs of signaling or deploying force, in particular through intelligent munitions, unmanned aerial vehicles, and ISR software.³² While the PLA's initial thinking on AI has been shaped by the analysis of U.S. military initiatives, Elsa Kania argues that the PLA may pursue a different path going forward based on its distinct strategic culture and organizational dynamics. In particular, Kania points out that the PLA has focused on the development of 'trump card' weapons which target vulnerabilities in U.S. battle networks, since the 1990s.³³

In a report published in 2017, Elsa Kania argues that the PLA seems to be "highly focused on the use of AI in simulation, war-gaming, and training, as well as to support situational awareness and command decision-making". The PLA's interest in using AI for simulation and training is related to its lack of combat experience, which means that simulations and computerized war-gaming already play a key role in its training; the PLA may therefore leverage AI to enhance the realism of such exercises. Regarding the use of AI to increase situational awareness and to facilitate command decision-making, the PLA is working on a variety of AI-based systems to autonomously fuse information from multiple intelligence sources into a single common operating picture.³⁴ In fact, the PLA has commissioned various projects which leverage deep learning to improve image recognition and differentiation of photographic, infrared, radar, and other sensor images.³⁵ At the same time, the PLA has prioritized the 'intelligentization' of its command information systems at the highest level and aims at developing intelligent assistance to command operational decision-making.³⁶ According to Morgan et al., the PLA hopes that these systems will in the future act as a "digital staff officer" which provides information, recommendations and planning suggestions to commanders.³⁷

At the same time, the PLA is aggressively developing autonomous robots.³⁸ To date, all branches of the PLA have started to field and deploy various unmanned systems of which some have at least a limited degree of autonomy.³⁹ In particular, China has invested heavily in the development of

³² Fediasuk, 2020, p. 2

³³ Kania, 2017, p. 4-5

³⁴ Kania, 2017, 4-5, 21, 29, 36; Morgan et al., 2020, p. 66 ; Morgan et al., 2020, p. 82

³⁵ Morgan et al., 2020, p. 66

³⁶ Kania, 2017, p. 29

³⁷ Morgan et al., 2020, p. 82

³⁸ Morgan et al., 2020, p. 62

³⁹ Kania, 2019, p. 31-32; Kania, 2021, 535

swarms of unmanned aerial vehicles (UAVs) and unmanned surface vehicles (USVs).⁴⁰ An example is the Blowfish A2 helicopter drone, which uses computer vision to recognize targets and can perform complex combat missions autonomously while also capable of forming a swarm.⁴¹ China has demonstrated its advances in swarming technology at various instances: In June 2017, the state-owned CETC tested a swarm of 119 fixed-wing UAVs, which engaged in catapult-assisted takeoffs and demonstrated complex formations;⁴² in December 2017, China set world records by testing a 1'180 quadcopter swarm at an air show in Guangzhou. Although the PLA appears to have invested less in the development of unmanned ground vehicles (UGVs) than in UAVs, it has still developed innovative systems such as Sharp Claw I, a six-wheeled, remote reconnaissance vehicle, and Sharp Claw II, a smaller armed UGV carried by the former. Moreover, the PLA has also developed maritime robotic systems and has reportedly already deployed the Jinghai USV, a small unmanned patrol boat capable of autonomous navigation and obstacle avoidance.⁴³

3. Russian strategic thinking on Artificial Intelligence

Like the Chinese leadership, Russia is considering AI to be a key technology for its future military capabilities. In a speech in 2017, Vladimir Putin publicly highlighted the importance of AI stating: “Artificial Intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world”⁴⁴ In recent years, the Russian Ministry of Defense has provided a consistent funding for AI R&D. The German software services company SAP estimated that the Russian state spent €343 million (US\$363.5 million) on scientific projects in AI between 2007 to 2017 corresponding to an annual investment of €34 million (US\$36 million). However, this figure falls way short behind the United States which spends around €189 million (US\$200 million) annually on AI research.⁴⁵ The structure of this chapter mirrors the previous chapter: It will first outline Russia’s national strategies and plans on AI development. Then, it will describe the Russian AI ecosystem. Lastly, it will discuss current and potential military applications of AI pursued by the Russian military.

3.1 National strategies and plans

The Russian government released its first formal proposal on AI, which included 10 recommendations for advancing AI in Russia, in March 2018.⁴⁶ As part of its ‘Digital Economy’ program, which was published in December 2018, the Russian government tasked Sberbank, a state-owned bank, which since 2011 has opened a technology branch Sberbank Technology, to draft a roadmap on the development of AI and neurotechnology. This AI roadmap was published in October 2019 and outlined relevant AI sub-technologies, such as natural language processing,

⁴⁰ Morgan et al., 2020, p. 61

⁴¹ Hynek & Solovyeva, 2022, p. 56

⁴² Kania, 2017, p. 23

⁴³ Morgan et al., 2020, p. 62-65

⁴⁴ “‘Whoever leads in AI will rule the world’: Putin to Russian children on knowledge day”, 2017

⁴⁵ Morgan et al., 2020, p. 91

⁴⁶ Hynek & Solovyeva, 2022, p. 62

speech recognition and computer vision.⁴⁷ It also estimates that a total of ca. €5.4 billion (392 billion rubles)⁴⁸ would be necessary for AI development through 2024. Already before the publication of the AI roadmap, Vladimir Putin instructed the government to develop a national strategy in AI. The national strategy, which was also drafted by Sberbank, was approved in October 2019 and should serve as the basis for planning and implementing state programs related to AI through 2030.

To accomplish the goals defined in the national strategy, the Russian leadership subsequently ordered the development of an AI federal project as an additional facet of the ‘Digital Economy’ program. The document, which was again drafted by Sberbank and approved by the government in August 2020, added funding and performance indicators to the goals set out in the national strategy and outlined a schedule for the development and implementation of AI schedules.⁴⁹ However, notably, no military-only strategy on AI exists yet in Russia.⁵⁰

3.2 Russian AI ecosystem

Russia’s AI ecosystem consists of clusters of interlinked activities between the government, state-owned enterprises, the military, academia, and the private sector. The key features of this ecosystem are that it is led by state-owned companies, and that a disproportionate amount of funding for the AI sector comes from the government. In 2018, 67% of funding for AI R&D in Russia came from the federal budget, whereas in the United States 77% of R&D funding respectively is provided by the private sector.⁵¹ As for China, it's difficult to distinguish between public and private sector funding. Moreover, Russian government has created incubators (e.g. the Skolkovo), funds (e.g. the Russian Direct Investment Fund) and initiatives (e.g. the National Technology Initiative) directed at facilitating the development of AI technologies. The Skolkovo Foundation, in particular, plays a central role in the Russian AI ecosystem as most R&D in the AI field is channeled through it. The Skolkovo Technology Park has become an institutional site for funding and hosting technology start-ups which also provides support for integrating start-ups into wider international markets. Apart from Skolkovo, important AI research hubs exist in clusters around state universities, notably the Moscow Institute of Physics and Technology, the Higher School of Economics, and the Far Eastern Federal University.⁵²

Furthermore, the afore-mentioned Sberbank plays a central role in the Russian AI ecosystem as it has been entrusted by the government with the development of all major AI-related national documents. At first glance, it might be surprising that the government has tasked a bank with drafting such documents. However, German Gref, the CEO and Chairman of the Executive Board of Sberbank, has adopted a strategy of turning the bank into a high-tech financial institution since assuming his position in 2007. With its ‘Strategy 2020’ presented in 2017, Sberbank launched its transformation into a universal technology company with its own ecosystem of financial and non-

⁴⁷ Edmonds et al., 2021, p. 20

⁴⁸ Conversion from rubles to Euro using the annual exchange rate in 2019 of €1 = 72.45

⁴⁹ Edmonds et al., 2021, p. 20-22

⁵⁰ Hynek & Solovyeva, 2022, p. 61

⁵¹ Nocetti, 2020, p. 21

⁵² Edmonds et al., 2021, p. 34, 63-64

financial services.⁵³ At the same time, the leading role of Sberbank in Russian AI development reflects the close ties between the company and the Russian government: The Ministry of Finance has a controlling stake in Sberbank owning 50% plus one share of the company, which it acquired from the Bank of Russia using funds of the National Wealth Fund in April 2020.⁵⁴ Moreover, there are connections on a personal level between Sberbank and the Kremlin. Sberbank's CEO German Gref is a long-time ally of Vladimir Putin.⁵⁵ Putin and Gref both worked in the local administration of St. Petersburg during the 1990s. During Vladimir Putin's first and second term as President, Gref served as Minister for Economic Development and Trade between 2000 and 2007.⁵⁶

Sberbank	
Corporate Structure & Shareholders	• Russian Ministry of Finance: 50% + 1 share • Domestic and International Investors: 50% - 1 share
Top Management	• Chairman of the Supervisory Board: Anton Siluanov (Russian Minister of Finance) • CEO & Chairman of the Executive Board: German Gref

Other key state-owned companies such as Rostec, Russia's most important defense conglomerate, or the energy companies Gazprom Neft and Lukoil are also working on a number of AI technologies but do not play an important role in the creation of the state's official AI strategy. Meanwhile, private technology companies play only a limited role in official government efforts to develop the AI sector. Yandex, Russia's largest technology company, has developed some AI products but has only played a secondary role in the development of Russia's AI ecosystem overall. Still, Yandex formed the 'AI Russia Alliance' together with other major companies such as Sberbank, Mail.ru, Gazprom Neft, MTS and the Russian Direct Investment Fund, which has successfully provided feedback for government initiatives.⁵⁷

Meanwhile, the Russian Ministry of Defense (MoD) also plays a key role in the AI ecosystem as a motor of innovation: Similar to the model pursued by the United States, in Russia the state acts as a capital provider for innovative civilian projects with military applications. Prioritized areas of technology include facial and speech recognition, imaging and neural networks. Within the Russian MoD, the Main Department for Research and Technological Support of Advanced Technologies and the Advanced Research Foundation are responsible for leading these initiatives. Since 2015, the Advanced Research Foundation, which possesses an annual budget of around €60 million and groups together 46 laboratories, has concentrated its efforts in particular on military robotics.⁵⁸

⁵³ Sberbank, n.d.; Sberbank, 2020

⁵⁴ "Government acquires Sberbank shares from Central Bank for \$29bln", 2020

⁵⁵ Edmonds et al., 2021, p. 25

⁵⁶ Munzinger-Archiv, 2022

⁵⁷ Edmonds et al., 2021, p. 63-67

⁵⁸ Nocetti, 2020, p. 24

Nevertheless, direct military-civil integration, as pursued by China, is relatively low at present.⁵⁹ Other organizations responsible for military aspects related to the development and application of AI include the MoD Commission for the Development of Robotic Systems for Military Purposes, which is led by Russian Defense Minister Sergei Shoigu, and the Main Research and Testing Robotics Center of the Russian MoD.⁶⁰ Moreover, military innovation is facilitated by Rostec and other defense enterprises.⁶¹ Lastly, the ERA technopolis, which was inaugurated in June 2018, will be a keystone for all developments in AI and other strategic domains such as cyber security and nanotechnology: On its campus near Krasnodar, the ERA technopolis brings together almost 600 researchers and 12 companies with plans to increase the number of researchers to 2000.⁶²

3.3 Military applications of Artificial Intelligence

Similar to China, Russia is pursuing AI R&D across a whole range of military applications. Yet, Edmonds et al. note that the Russian military is giving high priority and devoting significant funds to the development of aerial, ground and maritime unmanned robotic platforms and components.⁶³ During its military campaign in Syria, the Russian military has already tested its Uran-6 and Uran-9 UGVs. Moreover, Russia has conducted over 23'000 flight missions with unmanned aerial vehicles, mostly short and mid-range ISR drone platforms, in Syria.⁶⁴ While most of the unmanned vehicles tested by Russia are still remote-control, their level of autonomy may be scaled as the software improves.⁶⁵

Nevertheless, Russia's Military Industrial Committee has set a target to make 30% of its military equipment robotic by 2025. Morgan et al. consider this to be a very ambitious target considering the various obstacles Russia has faced when developing aerial unmanned systems. Notably, Russia has still not been able to field a medium-altitude long-endurance unmanned combat aerial vehicle.⁶⁶ Nocetti also notes that Russia has so far only developed prototypes of "intelligent" military robots, which possess AI-enabled control systems.⁶⁷ However, several Russian defense-industrial entities have tested AI-enabled combat drone platforms in the recent past: For example, in September 2019, the S-70 Okhotnik combat drone completed a first test of a loyal wingman flight alongside an Su-57 fighter aircraft. Moreover, Russia seems to be also particularly interested in swarm technology, especially in the maritime domain.⁶⁸ However, according to Morgan et al., the development of swarm technology lags starkly behind the United States and China.⁶⁹

⁵⁹ Edmonds et al., 2021, p. 38

⁶⁰ Hynek & Solovyeva, 2022, p. 66

⁶¹ Edmonds et al., 2021, p. 38; Hynek & Solovyeva, 2022, p. 66

⁶² Nocetti, 2020, p. 25

⁶³ Edmonds et al., 2021, p. 77; Morgan et al., 2020, p. 84

⁶⁴ Edmonds et al., 2021, p. 115-116

⁶⁵ Morgan et al., 2020, p. 84

⁶⁶ Morgan et al., 2020, p. 85

⁶⁷ Nocetti, 2020, p. 24-25

⁶⁸ Edmonds et al., 2021, p. 111-113, 118

⁶⁹ Morgan et al., 2020, p. 85

Notably, in 2018, Vladimir Putin also highlighted new semi-autonomous and possibly autonomous nuclear weapons which would supposedly be added to Russia's arsenal. Of those, only the Avangard hypersonic glide vehicle is already in service.⁷⁰ However, in January 2023, the Russian news agency TASS reported that Russia had also started production of the first set of its Poseidon autonomous underwater vehicles: The Poseidon resembles a torpedo, but is powered by a small nuclear reactor, which should give it unlimited distance, and has the potential for autonomous operation.⁷¹

Russia also has a long tradition in developing defensive systems with varying degrees of autonomy, which have been in service in Russia since 1979 when the Soviet Union constructed the world's first active protection system for armored vehicles. Its newest active protection system named Afghanit will be able to simultaneously detect and track up to 40 ground targets and 25 aerial targets and has already been added to T-14 Armata tanks. Similarly, the S-400 Triumph air defense system can autonomously detect and target up to 36 airborne threats at a distance of up to 250 kilometers. Moreover, in 2018, Russia began testing a new automated control system, which should unify the S-300 and S-400 air defense batteries, the Pantsir-S anti-aircraft weapons and radar systems under a single domain.⁷²

Furthermore, Russia has started to integrate AI elements into its command-and-control infrastructure, in particular its planning and decision-making support platforms; in fact, about half of Russia's state funding in the field of AI have been on data analysis projects (33%) and decision support systems (16.5%).⁷³ Russia's National Defense Management Center, which is tasked with continuous assessment and coordination of all domestic and international military and national security activity, reportedly already uses AI to collect and organize information. The Russian military level also intends to leverage AI at the operational level focusing on integrating information from different platforms across military branches to better coordinate forces and enhancing the speed of decision-making. At the tactical level, Russia is for example pursuing initiatives to develop onboard AI-enabled information and control systems in its fighter aircraft, which help to manage the flow of information available to the pilot.⁷⁴

Lastly, Russia may also leverage AI for a range of "gray zone activities" including cyber warfare, electronic warfare, influence operations, propaganda campaigns and disinformation. A prominent example is the use of AI to produce 'deep fakes'. Moreover, Russia has developed an automated electronic warfare system, the RB109-A Bylina, which can fully autonomously analyze combat situations, identify targets, decide how to disable them and ultimately send orders to electronic warfare forces in the field.⁷⁵

⁷⁰ Edmonds et al., 2021, p. 89, 91

⁷¹ Faulconbridge, 2023

⁷² Morgan et al., 2020, p. 86

⁷³ Ibid, p. 87-88

⁷⁴ Edmonds et al., 2021, p. 95-97, 103, 144-146

⁷⁵ Morgan et al., 2020, p. 88-89

4. Evolution of Russia-China cooperation in Artificial Intelligence

While the Russian government has generally highlighted its desire to collaborate with other countries in AI, Edmonds et al. note that partnerships with foreign companies have only played a limited role in the development of the Russian AI ecosystem. Apart from the sanctions imposed by the United States and the European Union on Russia from 2014 onwards, the limited engagement of Asian technology firms with the Russian market is rather due to its relatively small size and the lack of incentives for entrepreneurs to operate in the country.⁷⁶

An exception to this are the Chinese technology company Huawei and the South Korean firm Samsung, which have both established a strong presence in Russia. In fact, China has become Russia's most important partner with regards to high technology in general and AI in particular over the last years. Edmonds et al. consider this to be the result of increasing alignment of interests and security concerns based on a shared perception that Russia and China are in competition with the United States, and U.S. policy towards the two countries including sanctions, export controls and tariffs.⁷⁷

The following chapter will first outline the agreements underlying broader Sino-Russian cooperation on technology and innovation. Then, it will describe different areas of cooperation between the two countries. Subsequently, industrial cooperation between Chinese and Russian firms will be analyzed with a particular focus on Huawei's activities in Russia. Lastly, the limits of Russia-China cooperation in AI will be discussed.

4.1 Agreements underlying Russia-China technology cooperation

Technology and innovation have increasingly become a priority in the strategic partnership between China and Russia. Since Xi Jinping's state visit to Moscow in May 2015, the two governments have signed a series of agreements with the goal of expanding their cooperation into new fields, including the digital economy. Notably, the Chinese Ministry of Science and Technology and the Russian Ministry of Economic Development signed a 'Memorandum of Understanding on Launching Cooperation in the Domain of Innovation' in June 2016. Moreover, within the 'comprehensive strategic partnership, which Russia and China announced in 2019, the notion that the two nations are linked in a « science and technology cooperation partnership for shared innovation » has become one of the pillars of the relationship.⁷⁸

Although this notion has been primarily symbolic, the two governments have also launched various new forums and mechanisms to promote deeper collaboration including joint projects and partnerships among companies. Thus, the Russia-China cooperation in technology has gained in substance over time and has become increasingly institutionalized. While Russia and China are collaborating on a number of technologies, AI and robotics are among the sectors that have been highly prioritized in this technological cooperation.⁷⁹

⁷⁶ Edmonds et al., 2021, p. 153-156

⁷⁷ Ibid, p. 153-159

⁷⁸ Bendett & Kania, 2019, p. 5

⁷⁹ Ibid

Currently, the revenue that AI-related activity brings to Russia is growing 10 times faster than the country's GDP is growing. However, these statistics are negligible compared to Chinese figures, where investment in AI research is 350 times greater than in Russia. Moreover, China is second only to the US in the number of people employed in the AI sector. This is just one of many areas where the two countries have mutual interests and opportunities.

4.2 Areas of Russia-China technology cooperation

In a 2019 report, Bendett and Kania outline five areas where the Sino-Russian relationship is deepening: dialogues and exchanges, joint investment funds, the development of industrial science and technology parks, joint competitions and the expansion of academic cooperation.⁸⁰

The most important forum for exchange between Russia and China on technology is the Sino-Russian Innovation Dialogue, which takes place annually since 2017 and is jointly organized by the Chinese Ministry of Science and Technology and Russia's Ministry of Economic Development. In the first edition in 2017, over 100 Chinese and Russian companies from a range of industries including nanotechnology, robotics and AI participated. Moreover, in 2018, Russia and China signed the 2019-2024 China-Russia Innovation Cooperation Plan.⁸¹

Russia and China already opened a first joint science and technology park in 2006 in the Chinese city of Changchun. In June 2016, the plan for the China-Russia Innovation Park located in the Chinese province Shaanxi and funded by the Shaanxi Provincial Government, the Russian Direct Investment Fund and the Sino-Russian Investment Fund was announced. The park was opened in 2018 with IT, biomedical and AI enterprises invited to take part. Moreover, in 2017, science and technology parks from China and Russia announced to promote the construction of a Sino-Russian high-tech center at the Skolkovo Technology Park. In 2018, the Chinese city Harbin, which is located close to the Russian border, also unveiled an initiative to become a center for Sino-Russian technology cooperation.⁸²

Meanwhile, Russia and China have also increasingly invested in specialized funds for R&D in advanced technologies. For example, the Russia-China Investment Fund for Regional Development has become an anchor investor for two new funds at Skolkovo Ventures for €283 million (US\$300 million) in 2018. Most notably, however, Russia and China established the Sino-Russian Joint Innovation Investment Fund in July 2019 with an initial budget of €943.4 million (US\$1 billion). The fund is financed by the Russian Direct Investment Fund and the China Investment Cooperation and, amongst other things, will focus on financing AI research.⁸³

Cooperation between the Chinese and Russian technology sector has also been promoted through contests and competitions. For example, in September 2018, the first China-Russia Industry Innovation Competition took place, which highlighted big data, AI and high-end manufacturing.

⁸⁰ Ibid

⁸¹ Ibid

⁸² Bendett & Kania, 2019, p. 6; Edmonds et al., 2021, p. 160

⁸³ Ibid

Moreover, in July 2018, the Russian and Chinese academic institutions signed a roadmap agreement, which features a concentration on brain functions that will include elements of AI.⁸⁴

4.3 Evolution of Industrial Cooperation and the role of Huawei in Russia

Huawei has played a key role in commercial cooperation between Russia and China in high technology and in AI. Huawei opened its first research institutes in Moscow and St. Petersburg in 2017, which focused on developing mathematical models for communication technologies. In 2019, three additional centers were opened as Huawei announced that it would triple its R&D staff in Russia. In June 2019, Huawei acquired the rights to facial recognition technology developed by the Russian start-up Vocord for a reported €47 million (US\$50 million) and hired the majority of its staff. Moreover, the Chinese company signed a cooperation deal with Skolkovo and in November 2019, announced its plans to build an AI ecosystem in Russia comprised of 20 universities, over 100 software companies and more than 100'000 AI developers by 2025.⁸⁵

Huawei Technologies Co., Ltd. Huawei Holding & Investment Co., Ltd.	
Corporate Structure & Shareholders⁸⁶	Huawei Technologies Co., Ltd. - Huawei Technologies Co., Ltd. is a subsidiary of and fully owned by Huawei Holding & Investment Co., Ltd. Huawei Holding & Investment Co. Ltd. - Ren Zhengfei (founder & CEO): ca. 1% - Union of Huawei Investment & Holding Co., Ltd.: ca. 99%
Top Management⁸⁷	- Chairman of the Board of Directors: Liang Hua - Founder & CEO: Ren Zhengfei - Deputy Chairwoman of the Board of Directors & CFO: Meng Wanzhou (daughter of Ren Zhengfei)
Who really owns Huawei?	
According to the annual report of Huawei Investment & Holding Co. Ltd., Huawei is a “private company wholly owned by its employees”. Huawei Investment & Holding Co., Ltd., which is the parent company of Huawei Technologies Co., Ltd., only has two shareholders: Huawei’s founder Ren Zhengfei and the Union of Huawei Investment & Holding Co. Ltd. Through the latter, Huawei implements an “employee shareholding scheme”, in which 131'507 current employees or retired beneficiaries were involved as of December 31, 2021. The Union exercises shareholder rights through the Representatives’ Commission which elects Huawei’s Board of Directors and Supervisory Board. The Representatives’	

⁸⁴ Bendett & Kania, 2019, p. 7

⁸⁵ Edmonds et al., 2021, p. 161, Simes, 2020

⁸⁶ Huawei, 2022, p. 152-157

⁸⁷ Huawei, 2020, p. 152-157

Commission has 115 members, which are elected by the “shareholding employees with voting rights” on a one-vote-per-share basis.⁸⁸

However, Balding and Clarke argue that Huawei employees do not own actual stock in Huawei Technologies or Huawei Holding & Investment through, but only a kind of “virtual stock” that allows them to share in the profits. They therefore describe the “employee shareholding scheme” as “purely a profit-sharing incentive scheme”. As in China trade unions are accountable to superior trade union organizations – theoretically all the way up to the All-China Federation of Trade Unions, which is controlled by the CCP – Balding and Clarke argue that Huawei could be deemed to be a state-owned company.⁸⁹ Huawei has publicly dismissed these allegations stating that the Representatives’ Commission, which is distinct from the trade union committee, was the ultimate authority in the company.⁹⁰

Huawei’s cooperation projects are part of a broader strategy for the Russian market called ‘TIGER’. In the framework of this strategy, Huawei is concentrating on developing Russia’s AI system in three areas: Firstly, it plans to use its innovation laboratory Huawei OpenLab in Moscow to solidify cooperation with Russian companies in AI projects; secondly, it wants to train Russian developers as part of its global Ascend Development Community; thirdly, Huawei wants to develop courses related to AI technologies together with Russian universities. According to Edmonds et al., Huawei invested €4.7 million (US\$5 million) in partnerships in Russia in 2020 and plans to rise procurement from Russian suppliers from €370 million (US\$392 million) between 2017 and 2019 to €755 million (US\$800 million) between 2020 and 2025 while increasing the number of R&D centers in Russia to five.⁹¹

Notably, in 2020, Huawei’s Russian Research Institute established a joint R&D lab for AI and deep learning with the School of Applied Mathematics and Computer Science of the Moscow Institute for Physics and Technology (different from OpenLab : <https://career.huawei.ru/rri/en/>). The lab will concentrate on “developing neural network algorithms for computer vision, machine learning, and AI; developing methods for computational photography and image enhancement using mathematical modeling and advanced algorithms; and solving mathematically complex problems in order to create algorithms for simultaneous search and positioning”. This was already the tenth laboratory set up by Huawei in collaboration with Russian universities and research institutes, and it should not be the last, as the company plans to work with further Russian academic institutions through funding and partnerships.⁹²

Meanwhile, Huawei has also concluded various commercial partnerships with Russian companies. For example, Huawei is working with the Russian start-up VisionLabs to use its expertise in computer vision in the Huawei Atlas series of products for machine learning. Beyond AI, Huawei is also working with Russian firms in cloud computing. For example, it has established a partnership with the Russian cyber security company Kaspersky to use Kaspersky’s cloud security service in its

⁸⁸ Ibid

⁸⁹ Balding & Clarke, 2019, p. 10-11

⁹⁰ Li, 2019

⁹¹ Edmonds et al., 2021, p. 161-162

⁹² Ibid



FusionSphere cloud platform. Moreover, in March 2020, Huawei has signed a contract with Sberbank to launch a joint venture named “SberCloud.Advanced” targeting the Russian 5G market, which is a testimony to Huawei interest in developing the Russian technological ecosystem.⁹³

However, the Russian attack on Ukraine on 24 February 2022 and the following imposition of strict sanctions on Russia by the United States and the European Union have also affected Huawei’s business in Russia. In December 2022, the Russian newspaper *Kommersant* reported that Huawei would disband its Russian enterprise business group division, which is responsible for selling data storage systems and telecommunications equipment to corporate clients, on January 1, 2023, to avoid the risk of secondary sanctions. The around 2’000 employees of the unit will be reportedly asked to transfer to offices in other post-Soviet countries or will be laid off. However, Huawei’s R&D centers in Moscow, St. Petersburg, Nizhny Novgorod and Novosibirsk were not affected by the decision.⁹⁴

Apart from Huawei, other Chinese companies are also working with Russian firms in the field of AI. For example, the Chinese company Dahua Technology and the Russian start-up NTechLab presented a camera with facial recognition capabilities in May 2019, which they had jointly developed.⁹⁵ Notably, facial recognition software developed by NTechLab has been integrated by the city of Moscow in its network of CCTV surveillance cameras. While the software was initially supposed to help police investigations, it has been used to enforce quarantine lockdowns during the Covid-19 pandemic and it is expected that the system will also be used for counterespionage and political surveillance in the future.⁹⁶ Furthermore, the Chinese software developer Vinci Group has concluded an agreement with the Russian IT start-up Jovi Technologies to work on AI products.⁹⁷

NtechLab	
Corporate Structure, Shareholders & Investors	Shareholders⁹⁸ • Founders of the company: majority shareholders • Rostec State Corporation: 12.5% + 1 share (Note: According to a report by the U.S. magazine Wired, Rostec has sold its minority stake in the meantime)⁹⁹

⁹³ Ibid, Nocetti, 2020, p. 42

⁹⁴ Deng, 2022

⁹⁵ Nocetti, 2020, p. 41

⁹⁶ Edmonds et al., 2021, p. 69-70

⁹⁷ Edmonds et al., 2021, p. 164, Dimitri Simes, “Huawei plays star role in new China-Russia AI partnership,” Nikkei Asia, 4 February 2020, <https://asia.nikkei.com/Spotlight/Asia-Insight/Huawei-plays-star-role-in-new-China-Russia-AI-partnership>.

⁹⁸ Rostec, 2018

⁹⁹ Borak, 2023

	• Vardanyan, Broitman and Partners (VB Partners): 25% + 1 share (private investment company which manages the assets of Ruben Vardanyan and his partners)¹⁰⁰ • Impulse VC: undisclosed minority stake¹⁰¹ Other Investors • Russian Direct Investment Fund¹⁰² • Mubadala Investment Company (national wealth fund of the United Arab Emirates)¹⁰³
Founders	• Alexander Kabakov • Artem Kuharenko Note: According to a report by the U.S. magazine Wired, Alexander Kabakov and Artem Kuharenko both stepped down from NTechLab and left Russia in December 2021 and February 2022 declaring their anti-war stance on social media.¹⁰⁴

Zhejiang Dahua Technology Co., Ltd. (Dahua Technology)¹⁰⁵	
Corporate Structure & Shareholders	• Listed on the Shenzhen Stock Exchange Key Shareholders • Fu Liquan (founder): 13.37% • Shanghai Gaoyi Investment Management Co. Ltd.: 7.21% • Zhu Jiangming (Executive Vice President): 2.10% • China Securities Finance Corp. Ltd.: 2.07% • Chen Ailing (wife of Fu Liquan): 0.93%
Top Management	• Chairman of the Supervisory Board: Song Maoyuan • President & Director: Li Ke

¹⁰⁰ Vardanyan, Broitman and Partners, n.d.

¹⁰¹ "Russian billionaire invests in face recognition technology", 2017

¹⁰² Brewster, 2020

¹⁰³ Ibid

¹⁰⁴ Borak, 2023

¹⁰⁵ Factiva, 2023

4.4 Limits of Russia-China Cooperation

While the previous chapters have demonstrated that Sino-Russian cooperation in high technology and AI has increased in the last years, Bendett and Kania note that significant trust issues may still remain, which hinder Russia to adopt or acquire Chinese high-tech products.¹⁰⁶ Firstly, there is the long-standing grievance of Russian actors about intellectual property theft by Chinese actors.¹⁰⁷ However, according to Bendett and Kania, intellectual property concerns do not seem to be prevalent at the moment. Rather, Russian actors appear to be worried about the capture of Russian researchers and scientists by Chinese actors. For example, in 2019, the President of the Russian Academy of Sciences publicly expressed concerns that China was attracting Russian STEM talent with better pay and working conditions.¹⁰⁸ Apart from the capture of intellectual property and human capital, Russian elites also seem to be worried about the outflow of data from Russia to China.¹⁰⁹

Underlying all these considerations is the issue of the deepening technological asymmetry between the two countries, as Russian elites do not believe that China considers them to be an equal partner in AI and high technology. At the same time, Nocetti notes that parts of the Russian elite also see China as a role model for Russia regarding the employment of AI and other technologies for mass control and surveillance. Nevertheless, according to Nocetti, Russian experts consider any sharing of AI innovation in the military sphere to be the red line of Sino-Russian cooperation.¹¹⁰

Since leading Chinese technology companies like Huawei have reduced their exports to Russia out of fear of U.S. secondary sanctions, Russian technology companies increasingly have to rely on components and equipment produced by second tier and third tier Chinese manufacturers of inferior quality.

5. Case study: Covid-19 and mass surveillance

As mentioned in the previous section, parts of the Russian elite believe that China could serve as a model for their country regarding the use of AI and other technologies for mass control and surveillance. The Covid-19 pandemic and the sanitary measures adopted in response by Russia and China provide a useful case study to analyze in how far Russia has started to follow the Chinese model of mass control, and the repercussions it may have for the on-going Russia war effort. This chapter first outlines how China and Russia used digital surveillance tools in their response to the Covid-19 pandemic. After comparing the two cases, it is described how Russia has used its digital surveillance networks for mass surveillance and mobilisation since the outbreak of the war in Ukraine.

¹⁰⁶ Bendett & Kania, 2019, p. 14

¹⁰⁷ Nocetti, 2020, p. 43

¹⁰⁸ Bendett & Kania, 2019, p. 14

¹⁰⁹ Nocetti, 2020, p. 43

¹¹⁰ Nocetti, 2020, p. 43

5.1 Mass surveillance and Covid-19 measures in China

Already before the Covid-19 pandemic, China possessed the world's largest surveillance networks consisting of multiple local networks of more than 200 million CCTV cameras.¹¹¹ Most notably, China has deployed surveillance systems featuring extensive facial recognition technology in the Xinjiang Uyghur Autonomous Region where reportedly more than 170 million cameras were in use in 2018.¹¹² Moreover, the Chinese government has put great efforts into developing a national, unified social credit system. While a fully centralized social credit system is not yet in place, various individual systems are already operational, which rate, reward or punish citizens, businesses and government agencies based on their behavior.¹¹³

The Covid-19 pandemic and the CCP's emergency management response put this digital surveillance system, which combines facial recognition technology, security cameras in public and closed spaces, social media monitoring, telecommunications tracing, and the tracking of digital passenger information, on full display. At the same time, the pandemic allowed China to expand the use of surveillance technology domestically. For example, additional surveillance cameras were installed outside the front doors of houses and even inside residential buildings. Moreover, China deployed thermal temperature scanners and facial recognition technology at transport stations and other public places. The pandemic also spurred the development of new surveillance tools, which were used to combat coronavirus outbreaks. For example, the Chinese wearable technology company KC Wearable developed 'smart helmets', which can supposedly detect the body temperature of a passerby, scan QR codes for personal data, recognize license plates and identify people using facial recognition software.¹¹⁴

At the same time, China employed a contact-tracing app named "Health Code", which is fully embedded in widely used mobile platforms like WeChat and Alipay. The "Health Code" app assigns users a color-coded QR code (green, yellow or red), which determines if a person can travel or access public places.¹¹⁵ This color-coded QR code was derived from a person's answers to a questionnaire about travel and health history. In parallel, the Chinese government set up an "information big data travel card" using mobile data from the three largest telecom companies (China Telecom, China Mobile, and China Unicom) to monitor every person's travel history over the previous fourteen days.¹¹⁶ As the travel card information was interfaced with the health-code QR codes, the authorities could cross-reference the two data sources and thus prevent wrong or misleading information. While many other countries have used contact-tracing apps to combat the Covid-19 pandemic, Lo correspondingly argues that the Chinese "Health Code" app achieved an unprecedented level of tracking accuracy by automatically collecting a wide range of personal information.¹¹⁷

¹¹¹ Khalil, 2020, p. 10

¹¹² Lo, 2022, p. 1

¹¹³ Khalil, 2020, p. 11-12

¹¹⁴ Khalil, 2020, p. 14-17

¹¹⁵ Lo, 2022

¹¹⁶ Xu & Liu, 2021, p. 33

¹¹⁷ Lo, 2022

Khalil concludes that the pandemic provided a proof of concept to the CCP and the Chinese authorities that the technology works and that surveillance on a large scale and in an emergency is feasible and effective.¹¹⁸ Moreover, Lo argues that the Covid-19 pandemic may have changed the public's view of surveillance and led to the development of a "surveillance culture" as several studies found a high level of acceptance among Chinese citizens regarding contact-tracing and surveillance.¹¹⁹

5.2 Mass surveillance and Covid-19 measures in Russia

As in China, the Russian authorities made steps towards establishing large-scale surveillance systems before the Covid-19 pandemic. In particular, the capital city of Moscow served as a testing ground for digital city management technologies. In 2018, the Moscow Department of Information Technologies (DIT) presented its digital strategy for the city named "Smart City – 2030". The use of AI to analyze data from various sources and provide solutions to the government and businesses is a key element of this strategy. To provide data on the movement of inhabitants of Moscow, the DIT has been buying data from mobile operators, including SIM and tracking data, since 2015 while also using travel data from the Moscow Metro's travel cards, taxi trip logs, images from photo and video cameras, as well as data from public Wi-Fi networks. Even though the Deputy Mayor of Moscow, Maxim Liksutov, claimed that the city only received anonymized data, there are concerns that this data could be used to track the movement of specific persons.¹²⁰

At the same time, Moscow's municipal government progressively installed a large-scale video surveillance system. The system featured 178'000 cameras by the beginning of 2020, which is, however, still modest by world standards. From 2017 onwards, an AI-enabled facial recognition system based on the FindFace software by the Russian company NTechLab was integrated into the video surveillance system. Originally, the Moscow mayor's office argued that the video surveillance system primarily served safety concerns. In that regard, the 2018 World Cup served as the first real test of the system. During the tournament, 180 offenders listed in federal databases were reportedly detained and the system was subsequently expanded. By January 2020, the facial recognition system included 105'000 "smart" cameras.¹²¹

The Covid-19 pandemic allowed the Moscow authorities to further test and improve their digital control system and by the end of the lockdown it was operating without significant problems. First, in the middle of March 2020, the Moscow authorities started to monitor the SIM cards of individuals returning to Russia and send them text messages asking them to stay at home. On March 29, 2020, Moscow's mayor Sergey Sobyenin extended the stay-at-home regime to all residents of the city.¹²² To enforce this lockdown, Moscow's municipal government introduced a digital pass system on April 15, 2020: To leave their houses, citizens of Moscow had to register on a government website or app and declare a route and purpose; they then received a QR code, which could be checked by

¹¹⁸ Khalil, 2020, p. 19

¹¹⁹ Lo, 2022, p. 3, Xu Xu, 2022

¹²⁰ Markotkin, 2021

¹²¹ Ibid

¹²² Ibid

authorities.¹²³ After implementing the system in Moscow, the Russian government implemented the QR code enforcement technology across the country.¹²⁴ Moreover, on April 23, the Moscow DIT launched a “Social Monitoring” application to monitor infected individuals who were recuperating at home.¹²⁵

At the same time, at the height of the Covid-19 pandemic, the Moscow municipal government launched the “Safe City” surveillance network. “Safe City” builds on Moscow’s existing network of CCTV cameras. In addition to the information collected by the more than 200’000 cameras, it also uses data from 169 information systems including anonymized cell phone geolocation data, data from ride-hailing services, and voice recognition devices. By mid-March 2020, the facial recognition system of “Safe City” had reportedly already caught 200 people breaking lockdown restrictions. Apparently encouraged by these early results, the Russian government announced plans to invest around €1.2 billion¹²⁶ to deploy similar systems across Russia as “Safe City” was still being rolled out in Moscow. At the same time, Rostec has reportedly been working on further expanding the “Safe City” project by developing software that would help authorities to predict riots and prevent their escalation by analyzing media reports, data from social networks, video cameras, and other sources.¹²⁷

Even after most lockdown restrictions were lifted, key elements of digital surveillance including the facial recognition system and the use of geolocation data for tracking people’s movement remained.¹²⁸ Barros thus argues that the Kremlin, convinced of the system’s use, is making a country-wide push to expand control tools following the experiences of the spring 2020 lockdown.¹²⁹ For example, during the lockdown, Moscow’s role as a testing ground for digital technologies was further strengthened as the State Duma, the lower chamber of the Russian parliament, adopted a federal law in late April 2020 to create the conditions for the development and implementation of AI technologies in Moscow. The new law introduced an experimental legal regime – a regulatory sandbox – for the development of AI applications exempting authorities from data protection requirements.¹³⁰ In addition, on June 8, 2020, Vladimir Putin enacted a law establishing a unified register of information for Russian citizens, which will include, amongst other things, passport data, information on marital status, taxpayer information codes and family relations.¹³¹ Russian digital rights activists described the creation of this system as an attempt to obtain an “almost unlimited monopoly” on the collection and storage of biometrics.¹³²

¹²³ Ilyushina, 2020

¹²⁴ Barros, 2020

¹²⁵ Markotkin, 2021, p.3

¹²⁶ Conversion from rubles to Euro using the average annual exchange rate in 2020 of €1 = 82.73 rubles

¹²⁷ Borak, 2023

¹²⁸ Markotkin, 2021, p. 4

¹²⁹ Barros, 2020

¹³⁰ Markotkin, 2021, p. 2; Borak, 2023

¹³¹ Barros, 2023

¹³² Borak, 2023

5.3 Mass surveillance in Russia in the context of the war in Ukraine

In its response to protests against the war in Ukraine, the Kremlin can therefore draw on an established and tested digital surveillance system. In a review of more than 2000 court cases, the news agency Reuters found that Moscow's facial recognition video surveillance network played an important role in the arrests of hundred protesters most of who were detained in the aftermath of anti-government protests in 2021. Since the Russian invasion of Ukraine, Russian authorities have also started to use facial recognition to prevent people from protesting: According to data from the Russian human rights group OVD-Info, at least 141 people were detained preventively via facial recognition in 2022. They were detained by the police in Moscow metro stations on national holidays, when the authorities expected protests or at other times when anti-war sentiments were high. The Moscow metro uses a facial recognition system, named "Sfera", as part of its fare payment system and for security.¹³³

According to a 2021 news release on the city of Moscow's website, the Moscow metro has deployed algorithms from three Russian companies in its facial recognition system: NTechLab; VisionLabs, which is headquartered in the Netherlands, but owned by Russia's largest mobile operator, MTS; and Tevian, an AI company founded by staff from Moscow State University. This information corresponds to contracts published in 2022 on Russia's state tender website which show that Moscow's facial recognition system uses four different kinds of software: the LunaPlatform by VisionLabs, FindFace by NTechLab, FaceSDK by Tevian and a facial recognition software named Kipod developed by a fourth company, Synesis, from Belarus. Synesis is already under the U.S., EU and UK sanctions because of its role in suppressing pro-democracy movements in Belarus and Russia.¹³⁴

According to Reuters, these companies have also used U.S. technology for their software. NTechLab and VisionLabs have used graphics processing units (GPUs) by the U.S. company Nvidia and Synesis has used central processing units (CPUs) produced by Intel. Both Nvidia and Intel say that they have halted sales to Russia and Belarus since the invasion of Ukraine in February 2022. However, according to Russians customs records, at least 129 shipments of Nvidia products were imported to Russia between April 1 and October 31, 2022; of these, reports for at least 57 shipments stated that they contained GPUs.¹³⁵ Similarly, at least €431 million (US\$ 457 million) worth of Intel products were imported to Russia between April 1 and October 31, 2022. According to a joint investigation by Reuters and the think tank RUSI, Western computer components and electronics, which are subject to sanctions, continue to be imported to Russia via intermediaries in Hong Kong, Turkey and China.¹³⁶

5.4 Comparison of mass surveillance in China and Russia

Comparing the emergency response to the Covid-19 pandemic reveals parallels between China and Russia. In both countries, authorities relied heavily on digital technologies to enforce health

¹³³ Masri, 2023

¹³⁴ Ibid

¹³⁵ Ibid

¹³⁶ Stecklow, Gauthier-Villars and Tamman, 2022

measures. In this endeavor, large-scale video surveillance systems with AI-enabled facial recognition capabilities played a key role. Accordingly, both China and Russia used the pandemic to further expand the use of surveillance systems. Nevertheless, it should be noted that the quantity and density of surveillance cameras in Russia was and remains much lower than in China: In Russia, large-scale surveillance systems were limited to Moscow which serves as a testing ground for digital technologies. However, during the first wave of the pandemic in spring 2020, the Russian government took steps to implement digital tools such as QR code enforcement technology or video surveillance networks across the country. On a more fundamental level, the Covid-19 pandemic seems to have encouraged Russian officials – as it did their Chinese counterparts – that large-scale surveillance is both possible and effective. It is therefore no surprise that digital surveillance has also started to play a key role in the Kremlin’s attempts to quash protests against the war in Ukraine.

In April 2023, the Russian government furthermore rushed legislation through the parliament which allows the authorities to issue draft notices online via the state services website Gosuslugi and set up a digital database of all Russians eligible for military service. If a digital draft notice is issued and a person is failing to report to the recruitment office, they can be penalized. Penalties include a ban on leaving the country, as well as on driving, buying and selling real estate, taking out loans, and registering a small business. In other words, the system of digital control effectively closes off state borders to hundreds of thousands of individuals slated for mobilization. Meanwhile, the new digital database will collection information about possible draftees from every possible source including medical and electoral records, courts, and tax returns. According to Stanovaya, this new draft system is a first step towards establishing a digital system of societal control, which regulates individual access to rights and benefits based on political loyalty.¹³⁷

Within the Russian government, the Ministry of Digital Development will be responsible to build up to create the digital register foreseen in the new military conscription law. According to the news website Meduza, the Ministry of Digital Development will in turn task RT Labs, a subsidiary of Rostelecom, to build up this register. RT Labs has close ties to the Russian authorities. Russia’s Minister of Digital Development, Maksut Shadayev, is the former CEO of RT Labs. Meanwhile, RT Lab’s current CEO, Tengiz Alania, previously served as deputy director of Moscow’s Regional Center for Information and Communication Technologies. However, Meduza, cites a telecom industry insider stating that the Russian intelligence service FSB will oversee all the work carried out by the Ministry of Digital Development and Rostelecom.¹³⁸

6. Scenarios and recommendations

The inevitable systemic rivalry between the U.S. and China risks dividing the interconnected, globalized world, thereby stimulating the polarizing forces of bipolarity, with profound implications for the global system as a whole. The ensuing competition across all vital socio-economic systems will be dominated by the country that manages to achieve supremacy in the realm of AI-driven power. Although the U.S. will engage with China in applying AI across multiple domains, including

¹³⁷ Stanovaya, 2023

¹³⁸ “‘State Services R Us’ – Building a ‘digital gulag’ for draft-eligible Russians is turning into a major headache for the government IT contractor”, 2023

the economy, military, and society, the Chinese Communist Party's unique governance model creates a segment of the AI competition where the U.S., due to its systemic differences, has deliberately opted not to participate.¹³⁹ Undoubtedly, AI will be a pivotal catalyst for future warfare technologies, providing a significant edge to those who can extensively deploy it. The advent of autonomous weapons, AI-driven drones, advanced space and satellite technologies, and disruptive military hardware and software underscores that the digital revolution is an enduring phenomenon. It is poised to redefine the nature of warfare in unforeseen ways, leading to unprecedented ripple effects. It's indisputable that the competition for AI-powered military applications and technologies will profoundly influence the systemic contention between Washington and Beijing.

Given China's projected emergence as the most extensive domestic market for AI applications,¹⁴⁰ it's incumbent upon Washington to spearhead a robust alliance with ideologically aligned nations to cultivate a viable alternative to the AI market and create a substantial counterbalance to China's domination in this technological race. The U.S. will rely heavily on its transatlantic allies to bolster and diversify its AI expertise, while also aiming to construct a resilient alliance in the Indo-Pacific region to counter China's advancing technological footprint in this area. To preserve its long-term technological edge over China, the United States will have to nurture enduring partnerships with reliable and committed allies.

Two distinct scenarios lie ahead: a pessimistic one foresees a progressively comprehensive technological decoupling, while an optimistic one envisages a peaceful systemic coexistence, with Beijing focusing on fostering China-centric partnerships and commitments to bolster its domestic growth until it can counterbalance the overwhelming U.S. influence. Historically, the United States has played a pivotal role in China's ascent;¹⁴¹ however, it could equally trigger Beijing's decline through technological disengagement.

In the realm of AI, the Global AI Index (2021) ranks the U.S. and China first and second, respectively, based on an assessment of factors accelerating AI development: investment, innovation, and implementation. It signals the advent of a fierce technological arms race where AI is more than a technology; it's the future of technology itself.¹⁴² The entity that prevails in AI is likely to hold sway over global affairs, both economically and militarily. The implications for political economy, defense alliances, partnerships, and the impact on global norms and rules will be shaped by the speed, scope, and extent of advancements in this technological field. Over time, we may witness the emergence of two distinct supply chain networks - one revolving around the U.S.

¹³⁹ Allison & Schmidt, 2020.

¹⁴⁰ Allison & Schmidt, 2020.

¹⁴¹ Schell O. (2020, 3 April); The Ugly End of Chimerica; Foreign Policy.

<https://foreignpolicy.com/2020/04/03/chimerica-ugly-end-coronavirus-china-us-trade-relations/>

¹⁴² Armbruster A. (2020, 7 September) Wer in der KI führt, dominiert wirtschaftlich und militärisch; Frankfurter Allgemeine.

<https://www.faz.net/aktuell/wirtschaft/digitec/usa-gegen-china-ki-fachmann-zur-kuenstlichen-intelligenz-16942865.html?GEPC=s9>

and the other facilitated by China.¹⁴³ As Rajiv Malhotra underscores in his latest work, AI is the strategic lever that China is using to leapfrog the U.S. and achieve global dominance, making it the most sought-after pinnacle in the race for leadership in economic, political, and military affairs.¹⁴⁴

Moreover, disruptive technologies may not only amplify state control through mass surveillance but may also destabilize open democratic systems by upsetting fragile political balances. The tensions between China and India further muddies the pre-existing security dynamics in the Indo-Pacific region. Examples of fluid regional alliances due to ongoing systemic shifts include the growing closeness between China and Pakistan, and on a larger scale, between China and Russia (the Dragonbear).¹⁴⁵

The prospective digital alliances emerging from these geopolitical configurations remain uncertain. In a conflict escalation scenario, the U.S. would seize every opportunity to back New Delhi against Beijing, while Russia would seek to retain official neutrality, diplomatically mediating between the two sides. The geostrategic competition will predominantly play out in the South China Sea and the Indian Ocean, accentuating the tensions between the Asian giants and the competition between China and the United States. The culmination of the geostrategic rivalry between China and India remains undetermined, with both countries' approach reflecting a pragmatic blend of necessary cooperation and competition, including in the realm of Artificial Intelligence. Their relationship will be increasingly marked by economic and technological competition, geostrategic rivalry, and a risk to confront each other as they strive to mold their shared geoeconomic landscape. Looking forward, AI will be a critical determinant of the power balance.

Malhotra's concept of digital colonization is of increasing relevance, showcasing the tussle between the authoritarian governance model with a closed data market and the liberal governance model with an open data market. The political, ideological, and economic tensions within these different types of actors shape the geopolitics of technology.¹⁴⁶

Regarded as the world's largest digital democracies, Europe and India have demonstrated a stance against the questionable behavior of big tech firms, often restricted or even banned in authoritarian

¹⁴³ Tchakarova V. Is a Cold War 2.0 Inevitable?; Observer Research Foundation.
<https://www.orfonline.org/expert-speak/is-cold-war-2-inevitable/>

¹⁴⁴ Malhotra R. (2021) Artificial Intelligence and The Future Of Power: 5 Battlegrounds; Rupa.

¹⁴⁵ Tchakarova V. (2021) The Dragonbear: An Axis of Convenience or a New Mode of Shaping the Global System?; Irmo Brief.

<https://www.aies.at/publikationen/2020/the-dragon-bear.php> and

Tchakarova V. (2022a) Enter the 'DragonBear': The Russia-China Partnership and What it Means for Geopolitics, Observer Research Foundation.

<https://www.orfonline.org/research/enter-the-dragonbear/>

¹⁴⁶ Chaudhuri R. (2020, 4 December) India and the geopolitics of technology; The Hindustan Times.

<https://www.hindustantimes.com/analysis/india-and-the-geopolitics-of-technology/story-dd2DGyVvuhH7XmOfVSpLwL.html>

systems such as China. As AI becomes crucial in the global race for technological supremacy, Europe's and India's strategic choices and alliances will be instrumental in determining the outcome of the battle over digital dominion, leaning in favor of the governance model it supports.

The Guardian called data the oil of the twenty-first century.¹⁴⁷ In this context, AI emerges as a significant catalyst in the geopolitics of technology.¹⁴⁸ To thwart digital colonization, the U.S. and India are likely to collaborate, coordinating actions and measures against China's burgeoning influence. Despite concerns of inciting a "new Cold War" in light of ongoing Russia-Ukraine tensions and China's increasing military maneuvers in the Taiwan Strait, President Biden has upheld former President Trump's attempts to isolate China from global trade and technology networks. In 2022, the U.S. enacted the CHIPS Act to enhance domestic semiconductor production, bolster economic and national security, and target China.¹⁴⁹ This Act discourages recipients from expanding semiconductor manufacturing in China for a ten-year period after receiving the award. The U.S. Commerce Department's Bureau of Industry and Security (BIS) subsequently imposed export restrictions targeting China's development of critical technologies, particularly semiconductors. These measures illustrate the Biden administration's apprehension that advanced chips and equipment could facilitate China's development of new weapons and bolster its digital surveillance network.

Against this background, the bilateral Russia-China cooperation in the AI domain, which is part of a broad strategic partnership between Russian President Vladimir Putin and Chinese leader Xi Jinping, has been steadily increasing despite US and European attempts to hinder it through various sanctions. Samuel Bendett, who works at the Center for Naval Analysis and AI thinks that much of the cooperation between Moscow and Beijing takes place outside the defense sector. At the same time, the development of military ties provides new opportunities to establish more comprehensive cooperation and there is evidence of deepening bilateral contacts in the military sphere. Citing an example of an increased level of trust between the two countries, which in the past have repeatedly gotten into conflicts characteristic of the complex politics of the Cold War, Bendett points to Russia's assistance to China in creating an early warning system for missile launches.

The implications of such a relationship for U.S. strategy and the U.S.-Russia relations will become increasingly significant. The momentum with which Russia and China are building new AI systems has already alarmed some U.S. leaders and experts as the technical sophistication of the U.S. military is being challenged, particularly by China and Russia. Both countries are actively involved in the race for AI and could collectively overtake the Pentagon if it does not act decisively. However,

¹⁴⁷ Arthur, Charles (2013, 23 August). Tech Giants may be Huge, But Nothing Matches Big Data; *The Guardian*.

<https://www.theguardian.com/technology/2013/aug/23/tech-giants-data>

¹⁴⁸ Raibagi K. (2020, 10 November); *The Role Of AI Collaboration In India's Geopolitics*; Analytics India Magazine.

<https://analyticsindiamag.com/the-role-of-ai-collaboration-in-indias-geopolitics/>

¹⁴⁹ Calabrese J. (2022) CHIPS on the table: Escalating US-China tech war impacts the Mideast; *The Middle East Institute*. <https://www.mei.edu/publications/chips-table-escalating-us-china-tech-war-impacts-mideast>

cooperation between Russia and China in the field of AI is still at an early stage and many programs are less than five years old. At the same time, Edmonds notes that Russia and China have already surpassed the U.S. in terms of the scale of their collaboration." At this rate, it is hard to imagine that Washington would be able to sever those ties even if it tried. Amid rising tensions with the United States, China and Russia have clearly agreed to expand their technical cooperation, and AI plays a key role in their plans for the future.¹⁵⁰

In conclusion, cooperation in science and technology has become an important pillar of the 'comprehensive strategic partnership' between China and Russia. AI is one of the key technologies which has been highly prioritized in Sino-Russian technology cooperation. Moreover, as outlined in the case study on mass surveillance and Covid-19, Russia has followed the example of China and built-up a large-scale video surveillance system including facial recognition.

Based on this analysis, the final chapter of this reports outlines three – mutually not exclusive – scenarios for the future development of Sino-Russian technological cooperation and the deployment of digital surveillance technology in Russia in light of the war in Ukraine. Finally, the report will give recommendations on how France and the EU can respond to these scenarios.

6.1 Scenario 1 – Technological cooperation between Russia and China will increase because of the war in Ukraine

The first scenario concerns the trajectory of the technological cooperation between Russia and China. We can expect that Sino-Russian technological cooperation will increase because of the war in Ukraine – both on the governmental and at the company level. During Xi Jinping's state visit to Moscow in March 2023, he signed with Vladimir Putin a new bilateral agreement on cooperation in information technology and the digital economy. According to Soldatov and Borogan, this agreement contained significant, albeit unstated concessions on the side of Russia: in particular, Russian universities have become more open to Chinese students and researchers since the invasion of Ukraine. Most notably, Bauman Moscow Technical University, Russia's leading engineering school, agreed in July 2022 to join the Russian-Chinese university in Shenzhen, a joint venture launched by the Beijing Institute of Technology and Moscow State University in 2014.¹⁵¹

On the company level, Russian imports of electric machinery and parts as well as other dual use technology have increased since the invasion of Ukraine. According to data from Bruegel's "Russian foreign trade tracker", Russia imported €4.5 billion (US\$ 4.8 billion) in electronic machinery and parts from China in 2022, compared to €4.3 billion (US\$ 4.6 billion) in 2021. The data further shows that the imports of electronic machinery and parts by Russia from China plummeted from January 2022 onwards, but steeply increased again from June 2022 onwards.¹⁵² This increase occurred even though many leading Chinese technology companies like Huawei have reduced their export to Russia out of concerns over U.S. sanctions. Their place has, however been filled, by lesser-known Chinese companies with a much lower presence on foreign markets.

¹⁵⁰ Read the full story under this link: https://www.actualno.com/analysis/newsweek-rusija-syzdava-armija-ot-roboti-a-kitaj-j-pomaga-s-izkustven-intelekt-news_1599211.html

¹⁵¹ Soldatov & Borogan, 2023

¹⁵² Darvas et al., 2023

Notably, Chinese technology exports to Russia such as semi-conductors have often been routed through third countries like Turkey or the United Arab Emirates adding layers of protection for China from sanctions risks through intermediaries.¹⁵³ Despite these developments, however, any sharing of AI innovation in the military sphere will likely continue to be a red line for Russia in technological cooperation with China.

6.2 Scenario 2 – Russia will become increasingly dependent on Chinese technology

Meanwhile, increased technological cooperation also entails a growing dependency of Russia on Chinese technology. Increased technological independence in Russia could disrupt the global technology and geopolitical landscape if current trends continue.

Bloomberg recently reported on a memorandum drafted in the summer of 2022 by officials from the Russian Ministry of Digital Development, Communications and Mass Media, which reveals concerns among the Russian elites about their reliance on Chinese technology, in particular chips, network devices and electronics. The memorandum sets out concerns that having communications networks rely on Chinese companies such as Huawei may pose a danger to information security and network reliability. Moreover, the memorandum suggests that Russian officials are worried that their dependence on China may lead to diminished opportunities for domestic providers.¹⁵⁴

Accordingly, the memorandum provides a list of possible countermeasures to mitigate Russian reliance on Chinese technology and to promote the domestic production of critical equipment, including: imposing quotas on Chinese goods, pushing Chinese firms to shift production to Russia, demanding Chinese providers to use Russian nationals and sub-contractors, limiting the use of unbranded equipment, and incentives such as long-term contracts and subsidies for Russian developers and telecommunication companies.¹⁵⁵ However, in the past, attempts by the Russian military to replace foreign components with domestically produced parts in its weapon systems have failed. Under current circumstances, it is even more difficult to imagine that such attempts will be successful. Moreover, as the U.S. and the EU are increasing their efforts against sanctions circumvention, Russia may find it more difficult in the future to import U.S. and European computer and electronic components than in the first year of the invasion, which in turn limits Russia's leverage over China to zero. Therefore, it is likely that the Russian dependency on Chinese technology will only increase further relegating it to a 'junior partner' in its relationship with China.

6.3 Scenario 3 – Digital authoritarianism will expand in Russia

The third scenario concerns the use of digital tools for mass surveillance in Russia. As discussed in the case study in chapter 5, the Covid-19 pandemic allowed the Russian authorities to test and expand their digital control system. Furthermore, the Russian authorities learned to work with digital tools such as QR codes and quarantine violation monitoring via cameras and phone apps.¹⁵⁶ Finally,

¹⁵³ Seddon & Leahy, 2023

¹⁵⁴ Nardelli, 2023

¹⁵⁵ Ibid.

¹⁵⁶ Stanovaya, 2023



video surveillance systems equipped with facial recognition capabilities were expanded not just in Moscow, but also in the regions. These video surveillance systems remained in place after the pandemic and since the invasion of Ukraine have been used not only to arrest and detain anti-government protesters, sometimes even preventively, but also for mass mobilization of citizens through government services e-portal (which does not require the use of the portal application, or even owning a phone).

We should therefore expect Russia to take further steps towards digital authoritarianism. While today the most menacing use of digital surveillance is mobilization of eligible population, independent of their place of residence, the next step we can imagine is the use of surveillance for mobilizing citizens toward military economy, a scenario elaborated by Soldatov. The probability of digital economic GULAG increases with thousands of mobilized citizens in strategic companies, including but not limited to the military. Given that Russian elites consider China a role model for the use of digital tools for mass surveillance and control, Russian authorities may also establish a digital control system resembling China's social credit system. Reversely, China may learn from Russia's military mobilization experience to apply it to its own citizens in the scenario of Taiwan invasion.

All three scenarios are plausible directions for Sino-Russian relations in AI. However, Scenario 1: "Sino-Russian Technological Cooperation Amplifies due to the War in Ukraine" appears to be the most likely. Several factors suggest this.

First, the signed bilateral agreement during Xi Jinping's state visit to Moscow in March 2023 indicates a formal commitment to increase technological cooperation, including the AI domain. Second, there's been a demonstrated openness of Russian universities to Chinese students and researchers, a sign of increased collaboration in the realm of technology and research. Third, despite the U.S. sanctions and the initial dip in imports, Russia's imports of electronic machinery and parts from China have increased, showing a practical alignment in their tech sectors. Lesser-known Chinese companies complementing the tech giants like Huawei indicates a degree of resilience in Sino-Russian technological cooperation.

However, it is important to note that this scenario doesn't exclude the other two scenarios from eventually occurring. Increased technological cooperation with China (Scenario 1) may lead to increased Russian dependency on Chinese technology (Scenario 2), and also may contribute to a proliferation of digital authoritarianism in Russia (Scenario 3), following the example set by China's surveillance and control systems. These scenarios can occur concurrently or sequentially over time. It's also possible that new factors not considered in these scenarios could emerge and influence the trajectory of Sino-Russian AI cooperation.

As we look towards the future, several potential scenarios begin to emerge in the global security landscape. Firstly, we may witness the widespread adoption of AI in Quality Control across various defense industries. This could materialize if Russia's non-destructive quality control system, which leverages AI for inspecting semi-finished products and assembly units, is proven successful. Such an outcome may significantly improve the reliability and safety measures within defense industries globally, setting a new precedent in quality assurance.

Second, the nature of conflict dynamics could undergo a considerable shift. The surge in the integration of AI into military strategies is set to revolutionize warfare, transforming it into a more strategic and data-driven domain. Decision-making, previously based on human judgment and occasionally prone to error, could be augmented with AI's ability to analyze vast amounts of data quickly and accurately.

Third, the active and ongoing incorporation of AI into the military strategies of nations like China and Russia signals the advent of an AI arms race. This potential global competition would significantly alter power dynamics and necessitate an enhanced focus on AI-related defense capabilities. The imperative to remain competitive could drive nations to accelerate their AI research, development, and implementation in military applications.

Last, a greater reliance on commercial technologies in military operations could also be on the horizon. The trend of widespread adoption of these technologies, observed in the Russian war on Ukraine, may induce a strategic shift in future warfare. As commercially available technology continues to evolve rapidly, militaries worldwide might need to adapt and innovate quickly to integrate these advancements into their operational frameworks. This could lead to an increasing blurring of lines between civilian and military technologies, creating a new paradigm in the defense industry.

6.4 Recommendations

Based on these scenarios, the following recommendations can be made for the EU and France:

1. France and the EU should review and improve the sanctions on the export of dual-use computer and electronic components, such as chips, network devices and semi-conductors, to Russia. In particular, efforts are needed to ensure that sanctions are not circumvented via intermediaries in third countries such as Turkey, China (including Hong Kong) or the United Arab Emirates. Western dual-use technology not only plays a critical role in Russian weapon systems, but U.S. or European produced chips are also required for the development of facial recognition software employed by Russian authorities to detain anti-government protesters, sometimes even preventively. A system of value chain product tracing, sanctions implementation and penalties should in particular be revised and updated. While it requires significant investment, the cost can be shared with private actors, first and foremost equipment producers. Against this background, tightening the sanctions regime will likely further increase the dependence of Russia on Chinese suppliers.
2. Enhance Value Chain Tracing and Sanctions Implementation: It's crucial to upgrade the system for tracing product value chains and implementing sanctions. This implies developing robust mechanisms for tracking the end-to-end journey of dual-use technology. Collaboration with private actors, including equipment producers, is crucial in this regard.
3. Engage in Cybersecurity Dialogue and Cooperation: Given the proliferation of digital surveillance and control systems, the EU and France should actively engage in international dialogues about norms and regulations around digital surveillance, AI, and cybersecurity with like-minded partners. This could involve multilateral forums and direct negotiations with



countries like Russia and China, to promote transparency, accountability, and respect for human rights in the use of AI and digital surveillance technologies.

4. Establish national and European center of AI to observe and assess the activities of China, Russia and other potential competitors. Trace Russia's and China's advances in autonomous and robotic technologies, including usage of UAV's in military strategy and the potential transformation of commercial technologies such as DJI Mavic drones in conflict scenarios. Here are some instances of cooperation between China and Russia which should be watched closely and can be instrumental for the development of future sanctions against Russia:
 - a. Establishment of Joint Research Centers: The Moscow Institute of Physics and Technology (MIPT) and Huawei have set up a joint AI research center. This facility focuses on deep learning, decision-making algorithms, computer vision, and other AI-related advancements.
 - b. Sino-Russian University Collaboration: The Beijing Institute of Technology and Moscow State University jointly launched a Russian-Chinese university in Shenzhen in 2014. This joint venture focuses on the mutual exchange of students and researchers, fostering cooperation and advancement in fields like AI.
 - c. Belt and Road Initiative (BRI): Russia supports China's BRI, which is an ambitious plan to connect Asia with Africa and Europe via land and maritime networks. The initiative has significant technological aspects, including the enhancement of digital infrastructure and AI technology across participant nations.
 - d. AI Alliance Against COVID-19: Both Russia and China are using AI to combat COVID-19. They're sharing data and AI resources to develop better predictive models, improve diagnosis, and support vaccine development.
 - e. Joint Military Exercises: Russia and China have been conducting joint military exercises, such as the "Vostok" operation. These exercises involve sophisticated technologies, including AI-driven simulations and autonomous systems, indicating cooperation in the military domain as well.

While these examples demonstrate cooperation between the two countries, they do not necessarily imply the sharing of sensitive AI innovations, particularly in the military sphere, as both countries likely maintain certain reservations about fully sharing their advanced AI research and developments. For the most recent instances of Sino-Russian cooperation in AI, I would recommend consulting recent news articles, academic papers, or official government statements.

Conclusion:

As China progresses towards technological autonomy, it still seeks to integrate into the global science and technology space and engage in international cooperation. While China values Russia's contributions in basic science, Russia can learn significantly from China's success in commercializing R&D results. Russia and China have differing notions of technological

sovereignty. For China, it's about achieving the capacity to produce all key commodities, mastering core technologies, and being globally competitive. Conversely, for Russia, it's about acquiring fundamental technologies that can enable competition with the West and prevent lagging behind in development.

The country that will emerge victorious from the ongoing Fourth Industrial Revolution is yet to be seen, but the winner will certainly assert its dominance over both, competitors and allies, in the future by setting the new norms and rules in global affairs. Logically, there can be only one winner in such a decisive competition. Attempting to achieve dominance during the Fourth Industrial Revolution will require a quest for increased self-sufficiency in Artificial Intelligence (AI), critical technologies, and global supply chains. Inarguably, the battle for world domination will be between the U.S. and China, but Russia, EU and India's role will be critical to the final outcome.

Bibliography

1. Balding, C. & Clarke, D.C. (2019). *Who Owns Huawei?* (SSRN paper). Retrieved from: <http://dx.doi.org/10.2139/ssrn.3372669>.
2. Barros, G. (2020). Russia in review: Putin deploys new authoritarian controls during the Covid-19 pandemic. *Institute for the Study of War*. Retrieved from: <https://www.understandingwar.org/backgrounder/russia-review-putin-deploys-new-authoritarian-controls-during-covid-19-pandemic>.
3. Bendett, S. & Kania, E.B. (2019). A new Sino-Russian high-tech partnership: Authoritarian innovation in an era of great power rivalry. *Australian Strategic Policy Institute (ASPI) Policy brief Report No. 22/2019*. Retrieved from: <https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership>.
4. Borak, M. (2023, February 6). Inside Safe City, Moscow's AI Surveillance Dystopia. *Wired*. Retrieved from: <https://www.wired.com/story/moscow-safe-city-ntechlab/>.
5. Brewster, T. (2020, September 22). This Russian Facial Recognition Startup Plans To Take Its 'Aggression Detection' Tech Global With \$15 Million Backing From Sovereign Wealth Funds. *Forbes*. Retrieved from: <https://www.forbes.com/sites/thomasbrewster/2020/09/22/this-russian-facial-recognition-startup-plans-to-take-its-aggression-detection-tech-global-with-15-million-backing-from-sovereign-wealth-funds/#23045ef54b9e>.
6. Darvas, Z., Martins, C. & McCaffrey, C. (2023, April 25). Russian foreign trade tracker [Dataset]. Bruegel. Retrieved from: <https://www.bruegel.org/dataset/russian-foreign-trade-tracker>.
8. Deng, I. (2022, December 20). Huawei disbands enterprise business team in Russia in further pullback amid Western sanctions, local media reports. *South China Morning Post*. Retrieved from: https://www.scmp.com/tech/big-tech/article/3203995/huawei-disbands-enterprise-business-team-russia-further-pullback-amid-western-sanctions-local-media?module=perpetual_scroll_0&pctype=article&campaign=3203995.
9. Edmonds, J., Bendett, S., Fink, A., Chesnut, M., Gorenburg, D., Kofman, M., Stricklin, K. & Waller, J. (2021). *Artificial Intelligence and Autonomy in Russia*. Arlington, VA: Center for Naval Analyses. Retrieved from: <https://www.cna.org/our-media/newsletters/ai-and-autonomy-in-russia>.

10. New CNA REPORT from 2022 <https://www.cna.org/reports/2022/09/Artificial-Intelligence-and-Autonomy-in-Russia-A-Years-Reflection.pdf>.
11. Faulconbridge, G. (2023, January 16). Russia produces first set of Poseidon super torpedoes – TASS. *Reuters*. Retrieved from: <https://www.reuters.com/world/europe/russia-produces-first-nuclear-warheads-poseidon-super-torpedo-tass-2023-01-16/>.
12. Factiva. (2023). Factiva Company Report: Zhejiang Dahua Technology Co. Ltd. Retrieved from: <https://global.factiva.com/ar/arpdf.aspx?pp=PDF>.
13. Fedasiuk, R. (2020). Chinese Perspectives on AI and Future Military Capabilities. *CSET Policy Brief*. Retrieved from: <https://cset.georgetown.edu/publication/chinese-perspectives-on-ai-and-future-military-capabilities/>.
14. “Government acquires Sberbank shares from Central Bank for \$29bln”. (2020, April 20). *TASS Russian News Agency*. Retrieved from: <https://tass.com/economy/1142851>.
15. Huawei. (2022). *Huawei Investment & Holding Co., Ltd. 2021 Annual Report*. Retrieved from: <https://www.huawei.com/en/annual-report/2021>.
16. Hynek, N. & Solovyeva, A. (2022). *Chapter 3: Militarizing Artificial Intelligence in the US, Russia, and China*. In: *Militarizing Artificial Intelligence: Theory, Technology, and Regulation*, p. 49-84. New York: Routledge.
17. Ilyushina, M. (2020, April 14). Moscow rolls out digital tracking to enforce lockdown. Critics dub it a ‘cyber Gulag’. *CNN*. Retrieved from: <https://edition.cnn.com/2020/04/14/world/moscow-cyber-tracking-qr-code-intl/index.html>.
18. Kania, E.B. (2017). *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power*. Washington D.C.: Center for a New American Security. Retrieved from: <https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power>.
19. Kania, E.B. (2019). Chinese Military Innovation in the AI Revolution. *The RUSI Journal*, 164(5-6), 26-34. Retrieved from: <https://doi.org/10.1080/03071847.2019.1693803>.
20. Khalil, L. (2020, November 2). *Digital Authoritarianism, China and COVID*. Sidney: Lowy Institute. Retrieved from: <https://www.lowyinstitute.org/publications/digital-authoritarianism-china-covid>.
21. Larsen, B.C. (2019). China’s National AI Team: The role of National AI Open Innovation Platforms. In G. Webster (Ed.), *AI Policy and China: Realities of State-Led Development* (Stanford-New America Digichina Project Special Report No. 1) (p. 16-20). Retrieved from: <https://d1y8sb8igg2f8e.cloudfront.net/documents/DigiChina-AI-report-20191029.pdf>.
22. Li, T. (2019, April 29). Who controls Huawei? Chinese telecoms leader’s ownership structure explained in more detail. *South China Morning Post*. Retrieved from: <https://www.scmp.com/tech/tech-leaders-and-founders/article/3007863/who-controls-huawei-chinese-telecom-leaders>.
23. Lo, K. (2022). COVID-19 and the rise of the surveillance state in China. *Melbourne Asia Review*, 11. Retrieved from: <https://dx.doi.org/10.37839/MAR2652-550X11.5>; Xu Xu, Genia Kostka, and Xun Cao, “Information Control and Public Support for Social Credit Systems in China,” *The Journal of Politics*, 84:4, October 2022, <https://www.journals.uchicago.edu/doi/full/10.1086/718358>.
24. Markotkin, N. (2021). Does Coronavirus Herald the Age of Totalitarian Surveillance in Russia and Eurasia?. *Carnegie Endowment for International Peace*. Retrieved from: <https://carnegiemoscow.org/commentary/84044>.

25. Masri, L. (2023, March 28). Facial recognition is helping Putin curp dissent with the aid of U.S. tech. *Reuters*. Retrieved from: https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/?utm_source=Sailthru&utm_medium=Newsletter&utm_campaign=Weekend-Briefing&utm_term=041523.
26. Morgan, F.E., Boudreaux, B., Lohn, A.J., Ashby, M., Curriden, C., Klima, K. & Grossman, D. (2020). *Military Applications of Artificial Intelligence: Ethical Concerns in an Uncertain World*. Santa Monica, CA: RAND Corporation. Retrieved from: https://www.rand.org/pubs/research_reports/RR3139-1.html.
27. Munzinger-Archiv. (2022). Eintrag “Gref, German”. In *Munzinger Online/Personen – Internationales Biographisches Archiv*. Retrieved from: <https://www.munzinger.de/search/portrait/German+Gref/0/24915.html> [Own translation].
28. Nardelli, A. (2023, April 19). Russian Memo Said War Leaves Moscow Too Reliant on Chinese Tech. *Bloomberg*. Retrieved from: https://www.bloomberg.com/news/articles/2023-04-19/russia-china-worries-set-out-in-private-memo-on-tech-risk?cmpid=BBD041923_OEU&utm_medium=share&utm_source=website&utm_term=230419&utm_campaign=mobile_web_share.
29. Nocetti, J. (2020). Un outsider paradoxal : La Russie dans la course à l’intelligence artificielle. *Russie.Nei.Reports*, No. 34. Paris : Institut français des relations internationales (IFRI). Retrieved from : https://www.ifri.org/sites/default/files/atoms/files/nocetti_russie_intelligence_artificielle_2020.pdf.
30. Rostec. (2018, March 26). Rostec to Invest in Facial Recognition Technology [Press release]. Retrieved from: <https://rostec.ru/en/news/rostec-to-invest-in-face-recognition-technology/>.
31. “Russian billionaire invests in face recognition technology“. (2017, May 12). *East-West Digital News*. Retrieved from: <https://www.ewdn.com/2017/05/12/russian-billionaire-invests-in-face-recognition-technology/>.
32. Sberbank. (n.d.). SberBank history [Website]. Retrieved from: <https://www.sberbank.com/about/history>.
33. Sberbank. (2020, December 1). Sber presents Development Strategy 2023 [Press release]. Retrieved from: <https://www.publicnow.com/view/5BE04BA4EE76EAFFAE93969CBA44EB80A696CD68>.
34. Seddon, M. & Leahy, J. (2023, March 21). Xi Jinping-Vladimir Putin talks highlight Russia’s role as ‘junior partner’ to China. *Financial Times*. Retrieved from: <https://www.ft.com/content/73d50de6-53c8-4bf6-adf9-8cf108f82ca1>.
35. Simes, D. (2020, February 4). Huawei plays star role in new China-Russia AI partnership. *Nikkei Asia*. Retrieved from: <https://asia.nikkei.com/Spotlight/Asia-Insight/Huawei-plays-star-role-in-new-China-Russia-AI-partnership>.
36. Soldatov, A. & Borogan, I. (2023, March 23). China Finally Enters Russia’s Technological Treasure House. *Center for European Policy Analysis (CEPA)*. Retrieved from: <https://cepa.org/article/china-finally-enters-russias-technological-treasure-house/>.

37. Stanovaya, T. (2023, April 17). Russia's New Conscription Law Brings the Digital Gulag Much, Much Closer. *Carnegie Politika*. Retrieved from: <https://carnegieendowment.org/politika/89553>.
38. "'State Services R Us' – Building a 'digital gulag' for draft-eligible Russians is turning into a major headache for the government IT contractor". (2023, April 25). *Meduza*. Retrieved from: <https://meduza.io/en/feature/2023/04/25/state-services-r-us>.
39. Stecklow, S., Gauthier-Villars, D. & Tamman, M. (2022, December 13). The supply chain that keeps tech flowing into Russia. *Reuters*. Retrieved from: <https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-tech-middlemen/>.
40. Vardanyan, Broitman and Partners. (n.d.). About the Company [Website]. Retrieved from: <https://vbpartners.ru/en/about-the-company.html>.
41. "'Whoever leads in AI will rule the world': Putin to Russian children on knowledge day". (2017, September 1). *RT International*. Retrieved from: <https://www.rt.com/news/401731-ai-rule-world-putin/>.
42. Xu, F. & Liu, Q. (2021). China: Community Policing, High-Tech Surveillance, and Authoritarian Durability. In V.V. Ramraj (ed.), *Covid-19 in Asia: Law and Policy Contexts* (p. 27-C2.N100). Oxford: Oxford University Press. Retrieved from: <https://doi.org/10.1093/oso/9780197553831.003.0002>.