EGE Ecole de Guerre Economique

SURVEILLER.
ANALYSER.
PROTEGER.
INFLUENCER.

Rapport de Groupe

Russie : la Fédération en guerre.

« Economie de Guerre »

QUEST'IE 2025

AMADID Yunes, BARTH Alexandre, GOUTEYRON Pierre, Le DOYEN Baptiste, PFISTER Marc, ROUSSEAU Alexandre, SCATTON Lucas

EGE Ecole de Guerre Economique

Table des matières

EGE Ecole de Guerre Economique

Résumé exécutif

Héritière d'un complexe militaro industriel soviétique portant sur la puissance industrielle, la Russie a toujours compenser le manque de haute technologie par un pragmatisme efficient. A l'aune de la quatrième révolution industrielle, le pays tente de devenir aussi une puissance dans les domaines de l'intelligence artificielle, la robotique, le cyber et réalise des progrès et des produits notables. La montée en puissance de filière nationales prend du temps, et n'atteint pas les niveaux qui peuvent se trouver ailleurs ce qui fragilise structurellement le pays, déjà sous pression par la guerre. En effet, si la Russie s'appuie sur cette force par le bas, elle peine à acquérir des composants aujourd'hui critiques dans toute technologie. Une dépendance persistante aux composants électroniques étrangers via des importations parallèles, une fuite des talents, un manque de coordination entre acteurs limitent les initiatives. Malgré tout, la fusion civilo militaire fonctionne, que ce soit par l'intégration de groupes cybercriminels opérant au profit du Kremlin, ou la mobilisation de la société civile pour participer à l'effort de guerre par l'intermédiaire des campagnes de dons, des *Kulibins* avec le *Kulibin Club*, des centres de recherche et des écoles. Le cyber repose sur un écosystème à plusieurs cercles : services de renseignement (GRU/FSB/SVR) pilotant l'action, groupes cybercriminels souvent tolérés et parfois alignés tacitement, et entreprises privées/semi-étatiques fournissant des capacités défensives et des briques techniques, dans un modèle hybride public-privé propice au déni. L'IA est encadrée par une stratégie nationale actualisée (objectif « top 5 » mondial d'ici 2030), mais demeure marquée par un financement très étatisé, des retards d'infrastructures de calcul, et une logique de forteresse numérique qui favorise des champions locaux tout en limitant l'écosystème entrepreneurial. Côté robotique, l'industrie a accéléré dans une logique de « *prototype warfare* » avec une montée en cadence, l'intégration rapide d'acteurs publics et privés, des boucles courtes entre front et production, et transfert de technologies duales avec l'appui de coopérations extérieures (ex. production de *Shahed/Geran*) et des dispositifs d'innovation spécifiques. En somme, le système démontre résilience et unité globale du peuple pour répondre aux directives politiques que ce soit dans la mobilisation mais aussi dans les tâches de production ou soutien.

L'analyse du sujet a conduit à retenir trois champs principaux : intelligence artificielle, cyberespace, et robotique. La répartition s'est faite naturellement en fonction des expertises et intérêts de chacun, avec des binômes dédiés à chaque domaine. Le rapport est structuré en deux grandes parties ; pour chaque sous-partie, les contributeurs ont rédigé un paragraphe dans leur domaine afin d'assurer un traitement transversal et équilibré des trois champs. Le pilotage comprend la rédaction de certaines sous-sections, l'agrégation des contributions et la production des éléments de cadrage (introduction, résumé exécutif, conclusion). Le plan retenu vise à mettre en évidence la résilience et l'adaptabilité du secteur, ainsi que la mobilisation de la société civile dans l'économie de guerre.

Le travail recense 60 sources. La typologie est dominée par les rapports (23 sources, 38,3 %). Viennent ensuite les articles (17, 28,3 %). Les sources web représentent également un volume important (13, 21,7 %). On trouve enfin des formats plus ponctuels (10,1%) dont une interview (1, 1,7 %). Les sources anglophones sont les plus nombreuses (21, 35,0 %), suivies des sources russophones (15, 25,0 %) et francophones (11, 18,3 %). L'ukrainien représente 5 sources (8,3 %). Le reste est plus marginal et dispersé.

1 Introduction

Depuis février 2022, la Russie a adapté son outil industriel et technologique pour pouvoir soutenir l'effort de guerre. La structure et les évolutions de cet outil dans trois secteurs stratégiques que sont le cyber, l'intelligence artificielle, et la robotique mérite une attention particulière. Ces secteurs pâtissent depuis le début du conflit de sanctions successives. Malgré cela, on observe dans ces domaines une certaine résilience et parfois même des innovations, permettant ainsi à la fédération de Russie de poursuivre son effort de guerre. Cette résilience passe par une mobilisation très importante de la société civile et une culture de la « débrouillardise ». Par conséquent, comment la Russie exploite et adapte son secteur des nouvelles technologies dans le cadre de son économie de guerre ? Dans un premier temps, il conviendra de présenter l'écosystème technologique en Russie avant de mettre en lumière comment la société russe est entièrement consacrée à une économie de guerre.

2 L'écosystème technologique en Russie : Intelligence Artificielle, Cyber et Robotique

Les trois secteurs examinés mobilisent une multiplicité d'acteurs et de sources de financement. Bien qu'à des stades de développement différents, ils font face à des défis communs : des contraintes structurelles propres à leur domaine et des difficultés exacerbées par le contexte du conflit russo-ukrainien.

2.1 Panorama des technologie stratégiques russes

Le cyber russe est caractérisé par trois types d'acteurs. Le premier est constitué des services de renseignement russes qui structurent l'action cyber du pays : le GRU mène des APT (Active Persistent Threat) offensives (APT28 via le groupe Sandworm) pour le renseignement militaire et politique, le FSB utilise APT29 pour la sécurité intérieure et le contre-espionnage, alors que le SVR se concentre sur le renseignement extérieur et économique. Le Kremlin coordonne les objectifs stratégiques des services (annexe 1). Les seconds sont les nombreux groupes criminels comme Evil Corp, DarkSide/BlackMatter, Conti ou Ryuk (la plupart sont actifs dans le contexte de la Guerre en Ukraine ou ayant un fort impact dans leur milieu), et opèrent principalement à l'international avec une base opérationnelle en Russie et des proxys à l'étranger. Certains groupes agissent en alignement tacite avec l'État, ciblant l'Occident tout en respectant les « lignes rouges » du pouvoir russe afin d'éviter une confrontation directe avec l'Occident (annexe 2). Enfin, les entreprises privées ou semi-étatiques (Kaspersky, Positive Technologies, Rostelecom Solar, InfoWatch, RTSoft) fournissent des solutions défensives ainsi que des audits de sécurité, soutenant à la fois les administrations publiques et les infrastructures critiques souvent avec des liens ou un alignement stratégique avec l'État (annexe 3).

Cette volonté de maîtrise étatique, déjà démontrée dans le domaine de la cybersécurité, s'applique dans la course à l'hégémonie technologique avec l'intelligence artificielle.

En février 2024, la Russie a procédé à l'actualisation de sa « Stratégie nationale pour le développement de l'intelligence artificielle d'ici 2030 », affirmant ainsi ses ambitions de devenir un acteur majeur sur l'échiquier mondial de l'IA. Cette stratégie actualisée s'inscrit dans la continuité des orientations définies en 2016 autour des « grands défis » technologiques. Le secteur doit cependant composer avec une structure de financement déséquilibrée où 67 % de la R&D dépend encore du budget fédéral (contre près de 79% de fonds privés en Chine ou aux USA) et un niveau d'investissement deux fois inférieur à celui de la France. Cette stratégie a un objectif clair : positionner la Russie parmi les cinq puissances mondiales de l'intelligence artificielle d'ici 2030, derrière les USA, la Chine, le Royaume Uni, Israël et le Canada. Cela fixe des objectifs de rupture pour compenser les retards structurels avec le manque de datacenters ou de supercalculateurs marqués par une 46e place au *Global Innovation Index* en 2019.

Les objectifs chiffrés témoignent de cette ambition : une contribution de l'IA au PIB national estimée à 11,2 billions de roubles (11,6 % du PIB de 2024) ainsi qu'une multiplication par douze de la puissance de calcul nationale pour atteindre 6,2 Exaflops, soit la capacité d'effectuer 6,2 milliards de milliards d'opérations par seconde pour soutenir le développement de l'intelligence artificielle. Ce dynamisme se retrouve aussi dans un quintuplement du nombre de diplômés universitaires spécialisés, passant de

3 000 à 15 500 par an. Au cœur de cette stratégie figure le soutien aux centres de recherche en IA, avec un effort particulier sur les algorithmes d'apprentissage automatique et le développement de modèles de langage de grande taille (LLM). La Sberbank (dont 52 % du capital est détenu par l'État russe) confirme son rôle de pivot étatique du développement civil, pilotant l'effort sur l'IA. En effet, pour son PDG Guerman Gref, Sberbank n'est plus une banque dite classique, mais une « entreprise d'intelligence artificielle ».

Le paysage russe de l'intelligence artificielle s'organise donc autour d'un noyau d'acteurs industriels et institutionnels avec un niveau de maturité variable selon les secteurs. Sous l'égide du Ministère du Développement Économique (MOED), cette feuille de route lancée en octobre 2019 a été actualisée en février 2024 pour s'adapter à l'économie de guerre. Elle vise désormais à mobiliser 3600 milliards de roubles d'investissements privés d'ici 2030 pour garantir la souveraineté technologique.

La filière robotique russe connaît une profonde réorganisation, marquée par un resserrement des liens entre l'État, l'industrie de défense et des acteurs privés mobilisés dans une logique d'économie de guerre.

Face aux difficultés rencontrées dans la production de drone et dans l'approvisionnement du champ de bataille, les autorités russes n'ont eu d'autre choix que de se tourner vers de nouveaux acteurs de la défense, surtout dans le nouveau secteur stratégique du drone. Ces nouvelles synergies, portées par l'implication croissante des entreprises civiles et le recours accru aux technologies à usage dual, ont contribué à renforcer la production de matériels privés désormais intégrés aux dynamiques de guerre, brouillant progressivement la frontière entre drones civils et équipements militaires.

Les groupes industriels publics, notamment Rostec (incluant Kalachnikov et ZALA Aero) et Almaz-Antey, ont également dû augmenter leurs capacités de production, en particulier pour les drones d'attaque. Parallèlement, des entreprises privées comme Kronstadt (drones Orion), le centre scientifique et technique de Saint-Pétersbourg (Orlan-10), ainsi que de plus petites entreprises, ont été intégrées à l'effort industriel. En l'espace de dix-huit mois, plus de 520 000 emplois ont été créés dans l'industrie de défense (selon le Kremlin). Cette articulation entre industriels publics, acteurs privés et structures informelles marque une évolution du modèle. Raccourcissant les délais entre besoins opérationnels et production. Cette dynamique, bien que source de gains de réactivité, génère des fragilités en matière de standardisation et de gouvernance, compensées par une efficacité opérationnelle avérée au niveau tactique.

Ce changement de modèle se reflète dans les volumes et les capacités industrielles. Un accord conclu avec l'Iran début 2023 a permis l'implantation, au Tatarstan, d'un site de production de drones Shahed (Geran-2). La production mensuelle est ainsi passée d'environ 500 unités en 2022 à plus de 4 000 fin 2024. La société française Delair produit, de son côté, jusqu'à 50 drones par mois au maximum. À la mi-2025, la production de drones longue portée dépasserait 5 000 unités par mois, ce qui se reflète dans les frappes en profondeur sur les villes ukrainiennes. Cet effort est soutenu par des commandes publiques, une revalorisation salariale destinée à sécuriser la main-d'œuvre, et des dispositifs de financement spécifiques, notamment via la banque publique VEB. Le programme d'accélération « Voentech », lancé en 2025, vise à tester et intégrer rapidement les innovations issues du secteur civil dans les forces armées.

2.2 La montée en gamme des capacités technologiques russes dans un contexte d'économie de guerre

Cette évolution technologique s'exprime par de nouveaux fonctionnements entre les différentes strates de la société, mais aussi grâce à des nouvelles dynamiques relationnelles entre les différents blocs impliqués dans le conflit.

La période de 2022 à 2025 est marquée par une montée en gamme significative des capacités cybers russes et vers une intégration hybride (moyens privés publics et criminels) axée sur l'économie de guerre et la confrontation asymétrique avec l'Occident. Cette mutation des capacités cyber se décline de manière offensive et défensive.

Dans un contexte de guerre d'attrition avec l'Ukraine, les organisations cyber participant à l'effort de guerre ont adopté une approche plus furtive pour garantir leur persistance à long terme. Ainsi, l'espionnage traditionnel axé sur des malwares facilement détectables a pivoté vers une approche cloud avec l'attaque et l'infiltration de systèmes d'authentification (via le vol de token API d'interface Single Sign qui regroupe les accès à plusieurs applications, et l'infiltration du cycle Identity and Access Management qui gère l'accès, les privilèges et les rôles dans les systèmes d'information). Ce vecteur est plus discret et donc plus insidieux, tout en conservant une large surface d'attaque potentielle dans une économie prédominée par les Service as a Software (SaaS) et les solutions cloud, y compris dans le secteur public (11 000 institutions à travers le monde sont hébergées sur Amazon Web Services. La menace se caractérise également par l'usage de l'IA générative pour la création de contenus de phishing, l'amélioration de malwares et leur robustesse ainsi que pour appuyer un déni de responsabilité de campagnes futures. On constate globalement une extension du marché des Malware as a Service (MaaS) par IA avec WormGPT et FraudGPT pour la génération de mail de phishing. Cette croissance rend l'attribution d'attaques plus difficiles gardant une logique de déni des attaques tout en ouvrant des opportunités d'opérations type False Flag Operation, qui permet de masquer l'auteur réel des attaques.

La Russie a développé un arsenal juridique et technique important dans le cadre du contrôle de son réseau national : Loi sur l'Internet Souverain (Loi russe contrôlant internet, isolant Runet et contraignant les opérateurs à coopérer avec les autorités), GosSOPKA (Système étatique russe qui surveille et administre le trafic internet national en continu) et SORM (intercepte et analyse les communications téléphoniques internet au profit du FSB). Cet effort est axé sur la souveraineté numérique (*tsifrovoi suverenitet*), visant à garantir l'autonomie et l'indépendance de l'espace d'information national. Le RuNet constitue un premier effort du Kremlin. Cette isolation de l'internet d'un point de vue technique n'est pas entièrement effective mais demeure un moyen d'assurer la résilience interne, le contrôle de la population et une souveraineté des données tout en permettant à la Russie d'opérer avec un avantage asymétrique contre les adversaires qui maintiennent des réseaux nationaux ouverts. Cette asymétrie se caractérise par la vulnérabilité des réseaux occidentaux et la capacité de projection déséquilibrée en faveur des Russes. En 2024, c'est seulement 10 % du trafic Internet russe qui transite par des serveurs étrangers.

Dans cet espace numérique national isolé, l'autonomie ne repose plus seulement sur le réseau, mais sur des solutions logicielles d'intelligence artificielle développées par les géants locaux.

Les entreprises technologiques structurent le domaine : Yandex, avec *Alice* puis ses modèles souverains, et Sber avec *GigaChat*, occupent le segment des IA conversationnelles russophones. À leurs côtés, des acteurs spécialisés comme NtechLab, à l'origine de *FindFace* et des solutions Safe City, complètent l'écosystème.

Dans l'industrie lourde et les secteurs stratégiques, la maturité de l'IA russe apparaît surtout dans l'intégration de solutions opérationnelles. Gazprom Neft Illustre cette dynamique avec la plateforme *Cognitive Geologist*, qui applique le Deep Learning à l'interprétation sismique, et avec son programme Industrie 4.0 reliant IoT et pilotage automatisé de segment tel que l'exploration ou le raffinage. Rosatom intègre aussi des IA, en déployant par exemple des jumeaux numériques pour sa maintenance et en construisant des data centers associés à son parc énergétique. On observe donc des capacités solides en IA appliquée et en optimisation industrielle, mais des limites sur le calcul intensif. Au-delà de ces vitrines technologiques, la maturité de l'IA en Russie se heurte à une fracture numérique structurelle. Un fossé profond sépare les grands conglomérats d'État des PME et ETI où le faible niveau de numérisation des processus (dette technique, données non structurées ou silotées) rend le déploiement de l'IA inopérant. Si l'ingénierie russe excelle dans l'application et l'optimisation de technologies, elle peine davantage sur le plan de la recherche fondamentale en intelligence artificielle. Si Vladimir Poutine affirmait dès 2017 que « *celui qui deviendra le leader dans le domaine de l'intelligence artificielle sera le maître du monde* », la Russie reste aujourd'hui confinée à une position de suiveur technologique. Ce décalage s'explique par une dépendance critique aux calculateurs étrangers et une recherche fondamentale affaiblie, qui forcent l'écosystème russe à adapter des standards open-source internationaux faute de pouvoir générer ses propres algorithmes souverains.

Enfin, cette maturité est artificiellement soutenue par une stratégie de « forteresse numérique » où l'État joue un rôle de régulateur actif. Le Roskomnadzor (*Роскомнадзор*), le service exécutif fédéral russe chargé de la supervision dans le domaine des médias, finance des outils de surveillance automatisée comme le système *Oculus* créé par l'entreprise Eksikyushn, une IA de vision par ordinateur dédiée à la détection de contenus interdits à grande échelle. A titre d'exemple, selon les données révélées par le journal Vedomosti, Oculus permet désormais de traiter 200 000 images par jour, remplaçant la surveillance humaine pour traquer spécifiquement les caricatures du président Poutine ou la « propagande LGBT », tandis que le système complémentaire « Vepr » analyse la viralité de ces contenus pour prévenir les bombes informationnelles.

Cette dynamique s'inscrit dans le sillage de la «Loi sur l'Internet Souverain» de 2019 et s'est brutalement accélérée après février 2022, lorsque la désignation de Meta (Facebook, Instagram) comme organisation terroriste et extrémiste a vidé le marché de ses acteurs étrangers. Cette fermeture progressive du Runet génère un marché captif pour les champions nationaux. Ainsi, l'État garantit à VK (*VKontakte*), MAX ainsi qu'à Yandex, un accès exclusif aux données comportementales des citoyens, une ressource critique pour l'entraînement de leurs modèles souverains dans une logique d'autarcie technologique.

Depuis le début du conflit, le secteur du drone a évolué d'un usage principalement ISR (renseignement, surveillance et reconnaissance) vers des munitions rôdeuses, des drones FPV (First Person View) produits en série et bénéficiant de meilleures protections contre le brouillage.

La guerre électronique est désormais intégrée dans le cycle de conception, avec le recours à des sauts de fréquence, à la navigation inertielle et à la navigation sans GNSS, couplé à une formation de télépilotes plus exigeante (vol sans assistance). Des fonctions d'intelligence artificielle sont introduites de manière progressive, notamment pour l'assistance à la navigation, la reconnaissance de cibles et des formes limitées de coordination, sans autonomie décisionnelle complète. Malgré des dépendances résiduelles à des composants importés (annexe D), cette dynamique s'inscrit pleinement dans une logique de « *prototype warfare* », caractérisée par des boucles de rétroaction très courtes entre le front et l'industrie, une standardisation progressive et une adaptation continue des systèmes.

2.3 Difficultés et axes de tensions du secteur

Bien que les capacités cybers russes demeurent sophistiqués avec une projection de menace dans le temps, elles souffrent de plusieurs difficultés. La première est le manque de coordination entre les acteurs. En effet, malgré une complémentarité, les principales agences de renseignements sont en compétition constante et sapent l'efficacité globale du dispositif. On observe aujourd'hui que la majorité des cyberattaques russes n'utilisent que des versions actualisées d'anciens logiciels vulnérables et obsolètes, les exposant à une fragilité d'innovation et de prévisibilité.

Une autre contrainte opérationnelle majeure est la dépendance croissante aux acteurs proxys recrutés via le modèle de la gig Economy (recrutement de proxys en ligne) pour le sabotage physique. La faible qualité de ces proxys, souvent mal formés, rend leurs activités sujettes à la détection et à l'échec. Enfin, les sanctions occidentales coupant l'accès au système financier international ont entravé les opérations cybercriminelles à grande échelle. Les groupes criminels ont besoin de plus d'intermédiaires pour convertir leurs crypto-actifs en devises traditionnelles, ce qui augmente le coûts et le temps pour débloquer les fonds extorqués.

Ces fragilités cyber, nourries par des contraintes technologiques humaines et financières, témoignent d'un écosystème numérique sous tension. Elles se retrouvent dans le secteur de l'intelligence artificielle, pourtant présenté comme un pilier stratégique du pouvoir.

Le secteur de l'intelligence artificielle (IA) en Russie est confronté à des contraintes et des faiblesses notables, qui compromettent l'atteinte des objectifs stratégiques ambitieux fixés par l'Etat. L'obstacle le plus important est la dépendance chronique à l'égard de la haute technologie étrangère. La Russie dépend largement du matériel étranger, notamment les composants électroniques spécialisés qu'on peut trouver aux Etats-Unis, Taiwan, Singapour ou encore en Corée du Sud, essentiels pour la formation et l'exploitation des algorithmes d'IA. Les sanctions internationales ont considérablement entravé l'accès direct à ces composants critiques, tels que les GPU/accélérateurs IA de NVIDIA (famille A100/H100 et équivalents) et d'AMD (série Instinct MI, etc.), obligeant le pays à recourir à des importations parallèles via des pays tiers comme la Chine ou la Turquie, ce qui augmente les coûts et ralentit l'innovation.

La deuxième difficulté est le manque de travailleurs et la fuite des talents, qui constituent un obstacle structurel sérieux au développement de l'IA et de la robotique. De nombreux diplômés universitaires russes qualifiés dans l'IA cherchent des opportunités à l'étranger, en particulier en occident, attirés par des salaires beaucoup plus élevés. De plus, le retrait soudain des grandes entreprises informatiques internationales après février 2022, combiné à l'émigration accélérée des spécialistes de l'informatique,

affaiblit le paysage national de R&D. Enfin, la structure de l'écosystème russe, dominé par l'État, présente des inconvénients pour l'innovation. L'État domine l'économie russe via ses entreprises publiques (Rostec, Rosatom, etc...) et représente environ 50-60% du PIB indirectement selon des estimations d'avant 2022 (Banque mondiale). Cette centralisation décourage l'investissement privé et freine l'innovation en IA. Après une décennie de croissance économique inférieur à 1 % par an, le secteur privé reste affaibli par un climat d'affaires perçu comme instable, une protection juridique limitée et l'influence politique du pouvoir judiciaire. Dans ce contexte, le capital-risque demeure marginal, représentant moins de 0,02 % du PIB en 2023 (contre 0,4 % aux États-Unis), tandis que les start-ups d'IA peinent à lever plus de 150 millions USD par an, un chiffre sans commune mesure avec les montants observés dans les grands pôles mondiaux. L'accès restreint aux données et la prédominance des acteurs publics inhibent enfin la création d'un tissu entrepreneurial capable de soutenir l'innovation technologique autonome.

Le marché mondial des composants électroniques est le secteur dans lequel les sanctions s'appliquent le plus difficilement. Elles sont régulièrement contournées notamment pour la fabrication des drones Russes.

En effet, la plupart des technologies sont à usage multiple et produites à grande échelle. Ceci permet à la Russie de contourner les sanctions par des lignes d'approvisionnement utilisant des tiers, tels que la Chine, la Turquie ou des anciennes républiques soviétiques grâce à l'utilisation de ces biens à double usage. Selon la Kyiv School of Economics, 91 % des composants étrangers identifiés dans des drones russes proviennent d'entreprises situées dans des pays appliquant des sanctions, dont 69 % à capitaux américains. Malgré les restrictions, les importations russes de semi-conducteurs sont passées de 1,82 Md$ en 2021 à 2,45 Md$ en 2022. Ces composants sont souvent moins adaptés à leurs usages et proposent des performances dégradées mais suffisantes. Ces mécanismes reposent sur la réexportation rapide, la dilution de la traçabilité et la banalisation de standards industriels peu contrôlables. À court terme, cette recomposition permet de maintenir une capacité de production militaire, mais à moyen terme l'isolement technologique, la fuite des compétences et la dépendance accrue à des substituts imparfaits fragilisent structurellement l'industrie technologique russe et accroissent les risques juridiques et réputationnels pour les acteurs occidentaux. Néanmoins, cette dépendance peut démontrer un autre aspect. Entre le Geran 2 et 3 la quantité de composants étrangers recensés tombe de 75 à 45. Ces chiffres peuvent impliquer plusieurs hypothèses, soit le matériel est moins performant et nécessite moins de matériaux, soit la Russie parvient à construire sa propre industrie. Dans ce deuxième cas de figure, la dépendance sert d'alternative le temps de développer son propre parc d'usine.

3 La société civile russe impliquée dans l'effort de guerre

3.1 Un système de formation au service de l'appareil militaro-technologique

Afin de construire ce secteur d'activité stratégique, la Russie a besoin de personnel qualifié pour servir l'effort de guerre. C'est pourquoi le système éducatif russe est marqué par une orientation croissante vers la formation d'une génération prête au combat et qui maîtrise les nouveaux outils.

Dans le domaine de la formation au drone il est important de noter que depuis septembre 2024 les élèves de quatrième et de troisième (8ème et 9ème année dans le système scolaire russe) ont accès au

manuel Unmanned Aerial Vehicles**:** publié par *Geoscan* un fabricant de drone russe. Ce manuel est utilisé comme support de cours pendant un module de 34h lors des cours de technologies. La publication de ce livret s'inscrit dans un projet fédéral de formation à l'usage du drone. La fédération de Russie a prévu d'entraîner 1 millions d'opérateurs drones dans plus 500 écoles et 30 universités du pays d'ici à 2030. Pour ce faire, en 2024, Moscou a acheté 18 000 drones pour un total de 8,38 milliards de roubles. On observe également sur l'ensemble du territoire la multiplication des écoles de formation au pilotage à la construction et à la programmation de drone, couplée à des polygones d'entraînement au vol sans GNSS. L'une des initiatives la plus marquante est l'école *Dobro y nebo* (gentillesse et ciel) pour adolescents de 14 à 18 ans ayant ouvert le 26 septembre à Krasnodar. L'école a été créée par la fondation locale *dobro i nelo* (gentillesse et action) et propose des cours gratuitement grâce au soutien du gouverneur local pendant 9 mois et délivre un certificat d'état à l'issue de la scolarité. La formation est dispensée par une majorité de vétérans de la guerre en Ukraine. Les élèves apprennent le pilotage sur simulateur et en situation réelle mais également, la programmation, la construction et la conception de drone notamment grâce à des imprimantes 3D.

Concernant l'intelligence artificielle, les universités jouent un rôle très important dans le développement de solutions civiles et militaires. Récemment cinq universités russes ont rejoint le programme de Yandex Education appelé « physical IA garage » HSE University, ITMO, MIPT, MAI, MEPhI. Le but de ce programme et de de développer l'IA physique c'est à dire capable de percevoir son environnement, l'analyser et prendre des décisions. Ce projet concerne les domaines industriels mais aussi le domaine des systèmes autonomes. La Russie voit depuis 2008 l'intelligence artificielle comme un outil permettant de rattraper les puissances occidentales dans la modernisation de son armée. Les formations en intelligence artificielle en Russie sont nombreuses et certaines ont des laboratoires particulièrement intéressants pour le domaine de la défense. C'est le cas de la MIPT (*Moscow institute of physics and technologies*) qui héberge le *Neural Networks and Deep Learning Lab* un laboratoire spécialisé en réseaux neuronaux et apprentissage profond, qui fait partie des principaux centres de recherche et développement en IA identifiés comme critiques pour les besoins militaires du complexe militaroindustriel. Ces structures sont incluses dans l'écosystème russe de R&D en IA directement relié à des priorités de défense comme le commandement et contrôle, la reconnaissance automatisée et les systèmes autonomes. On peut également citer le *Skolkovo Institute of Science and Technology (Skoltech)* qui a signé un partenariat avec Rostec portant sur des programmes de recherche et de formation en technologies avancées (incluant des systèmes autonomes, l'IA et la robotique).

Dans un contexte d'intégration des besoins étatiques, la Russie déploie de plus en plus de moyens dans le secteur du cyber au sein de son système éducatif.

La Russie bénéficie d'une synergie d'acteurs assurant la formation et l'exploitation des talents cyber du pays. Parmi les plus grands acteurs, on peut citer *Security Code*, une société de cybersécurité, spécialisée dans les technologies et services défensifs ; elle entretient des partenariats éducatifs avec des universités publiques et privées russes. De plus, le FSB est réputé pour son recrutement de personnel cyber depuis l'université nationale de recherche nucléaire (MEPhI). La relation inverse existe aussi, l'institut académique de cryptographie, de communication et d'informatique du FSB (IKSI) affirme être partenaire de plus de deux cents institutions éducatives. De plus, l'IKSI assure que des membres de son corps professoral incluent des professeurs des meilleures universités russes, notamment la MEPhI. En plus de partenariats entre le privé et les universités, ces universités, telles que la MEPhI et l'université nationale de recherche (MPEI), soutiennent les objectifs militaires du gouvernement russe. Le MPEI gère par exemple un centre de formation militaire pour les forces

aériennes et spatiales russes. Enfin, l'université possède un institut d'ingénierie militaire visant à « renforcer l'interaction avec les universités du ministère de la Défense russe » et a signé un partenariat avec la technopole militaire innovant « ERA » (infrastructure du ministère de la Défense) pour développer des technologies pour des produits militaires et à double usage, notamment pour contrer les cybermenaces.

3.2 L'utilisation duale civil-militaire comme stratégie structurelle de mobilisation

La Russie pratique une fusion civilo-militaire décomplexée où l'État oriente la R&D civile vers un usage dual. Le ministère de la Défense (MOD) intègre ainsi directement la vision par ordinateur de Sber et Yandex, afin de rationaliser les ressources disponibles. De même, la reconnaissance faciale de NtechLab (système *Safe City*) est réadaptée pour l'identification de cibles en zone de conflit.

Le système de guerre électronique RB-109A Bylina, grâce au machine learning, hiérarchise les cibles en temps réel, augmentant l'efficacité du brouillage de 50 % par la suppression des délais humains tout en gardant la prise de décision humaine dans la boucle. Cependant cette technologie reste limitée et peu opérationnelle. En 2023 l'armée ukrainienne a publié une vidéo montrant la destruction d'un de ces véhicules suite à sa détection par un drone avant d'être ciblé par l'artillerie ukrainienne.

Cette autonomie s'étend aux munitions rôdeuses Lancet (ZALA Aero, filiale du groupe Kalachnikov), bien qu'elle comporte des limites : le guidage terminal autonome par IA repose sur un verrouillage visuel préalable de la cible («pixel lock»). En cas de brouillage, le drone maintient sa trajectoire vers l'objet verrouillé, mais ne chasse pas de manière totalement automatique sa cible sur une portée infinie. Enfin, au niveau tactique, si les drones Eleron-10 et Granat-2 (UV2) calculent les coordonnées via leurs algorithmes embarqués, l'optimisation des frappes provient surtout du logiciel de Commandement et de Contrôle (C2), qui serait potentiellement le système «Planshet-A» présenté lors du salon Army 2023 qui permet de détecter les positions d'artilleries ennemies à une distance pouvant atteindre les 38 km. Ce dernier retranscrit ces données sur une cartographie GPS, transmettant ainsi directement des coordonnées de tir exploitables aux artilleurs en cas de brouillage.

Le développement de ces technologies clés poursuit un rythme soutenu. Celui-ci se caractérise par l'entrée dans le secteur de nombreux acteurs indépendants directement intégré au cycle de l'innovation.

3.3 La culture *Kulibin* : innovation improvisée et adaptation en temps de guerre

Les *Kulibin* sont au cœur du cycle de l'innovation en Russie. Ces inventeurs improvisés sont devenus une pièce maîtresse de l'innovation en Russie, notamment grâce aux programmes étatiques qui favorisent leurs activités. Le choix de l'appellation « *Kulibin* » renvoie à une référence culturelle russe. Ivan Koulibin, inventeur autodidacte du XVIII^{e} siècle, incarne la figure de l'ingénieur populaire capable de produire des solutions efficaces en dehors des cadres industriels et académiques. Cette référence participe à une narration valorisant l'autonomie technologique nationale et la contribution directe de la société civile à l'effort de guerre.

Dans ce cadre, il est important d'évoquer le *Kulibin Club*. C'est une initiative lancée en décembre 2024 par le Front populaire russe (ONF) afin de capter, structurer et orienter l'innovation technologique civile au service des forces armées russes dans le cadre de la guerre en Ukraine. Le dispositif repose sur un réseau d'inventeurs, d'ingénieurs indépendants et de petites équipes techniques réparties sur

le territoire russe. Ces acteurs sont invités à proposer des solutions répondant à des besoins opérationnels identifiés sur le terrain. Les projets sélectionnés font l'objet de tests, d'adaptations et, le cas échéant, d'une mise en production rapide avec l'appui logistique et institutionnel de l'ONF. Les domaines couverts concernent principalement les drones, les systèmes de lutte anti-drones, la guerre électronique, la robotique terrestre et certains équipements de soutien.

Sur le plan institutionnel, le *Kulibin Club* bénéficie d'un soutien explicite de l'État. Intégré aux initiatives nationales de mobilisation telles que « Tout pour la victoire », il agit comme une interface entre innovation civile, besoins militaires et structures publiques. Sans se substituer à l'industrie de défense, il permet de contourner certaines inerties bureaucratiques en accélérant les cycles de développement et de déploiement de solutions à faible coût et à forte utilité tactique.

Le *Kulibin Club* illustre ainsi une évolution pragmatique de l'approche russe de l'innovation en contexte de guerre. En s'appuyant sur des compétences civiles, en favorisant l'expérimentation rapide et en maintenant un lien direct avec les unités engagées, ce dispositif contribue à l'adaptation tactique des forces russes face à un environnement technologique et opérationnel contraint, marqué par les sanctions et la pression industrielle.

Une autre illustration de cette culture peut être observée dans le domaine du cyber. En effet, les attaques complexes demandant de gros moyens techniques deviennent impossibles à réaliser à grande échelle par les acteurs russes. Au début de la guerre en Ukraine, les services russes avaient lancé une série d'attaques techniquement complexes contre les infrastructures électriques, gouvernementales et médiatiques ukrainiennes (groupe Sandworm, APT 28). Ils se concentrent désormais sur des attaques plus simples, moins intenses et à moindre échelle, comme les *DDoS* (*deny of service*). Une analyse du Centre des études internationales et stratégiques (CSIS) a conclu que malgré l'augmentation significative (75%) du nombre d'attaques après l'invasion, leur sévérité a drastiquement baissé.

4 Conclusion

L'écosystème technologique russe illustre une transformation profonde, où l'innovation et la production dans le cyber, l'IA et la robotique sont directement orientées vers les besoins militaires. Au cœur de cette dynamique, la société civile joue un rôle clé : les inventeurs *Kulibin*, les start-ups, les universités et même les élèves sont intégrés dans un continuum éducatif et industriel visant à former et exploiter des talents pour l'effort de guerre.

L'État centralise et coordonne cette mobilisation, mais elle repose sur une combinaison unique d'initiatives publiques, privées et informelles, accélérant l'adaptation des technologies civiles à des usages militaires. Grâce à cette approche le cycle de l'innovation est plus rapide, l'État identifie l'innovation qui l'intéresse puis la produit à grande échelle. Discriminant dans le même temps les solutions les moins prometteuses.

Pourtant, malgré cette mobilisation totale, la dépendance aux composants étrangers, la fuite des talents et les limites structurelles de l'écosystème freinent la souveraineté technologique. La Russie apparaît ainsi capable d'une innovation tactique et d'une mobilisation sociale exceptionnelles, mais sa puissance technologique globale reste fragile à moyen terme.

Le conflit permet à la Russie de tester sur le terrain de très nombreuses innovations gagnant ainsi une avance considérable dans le combat du futur en formant d'ores et déjà la nouvelle génération d'utilisateurs.

5 Annexes :

Annexe A :

Acteurs étatiques cyber en Russie

Acteur Étatique	Service de Renseignement Affilié	Groupes APT Notables	Objectifs Principaux
GRU (Direction Principale de l'État-Major)	Renseignement militaire	APT28 (Fancy Bear, Strontium, Pawn Storm), Sandworm, Gamaredon	Renseignement politique, renseignement économique, opération de terrain, contre renseignement
FSB (Service Fédéral de Sécurité)	Sécurité intérieure et contre-espionnage	APT29 (Cozy Bear, The Dukes, Nobelium)	Renseignement politique, opération de terrain, contre renseignement, sécurité politique, enforcement de la loi
SVR (Service de Renseignement Extérieur)	Renseignement extérieur	APT29 (partiellement, chevauchement avec le FSB)	Forte propension au renseignement politique et économique, renseignement militaire, opérationnel, contre renseignement, securité politique
Sources : NATO StratCom COE			

Sources : **NATO StratCom COE**

Annexe B :

Groupes cyber-criminels en Russie

Groupe Criminel	Cibles et Activités Principales	Lien avec l'État/Particularités
Evil Corp	Ransomware (WastedLocker), Fraude bancaire (Dridex). Ciblage d'organisations occidentales alignée OTAN.	Liens étroits présumés avec le FSB selon le Trésor américain. Leur leader, Maksim Yakubets, est recherché par le FBI.
DarkSide / BlackMatter	Ransomware-as-a-Service (RaaS) pour des attaques très médiatisées comme Colonial Pipeline et Toshiba	Bien que purement criminels, ils évitent systématiquement d'attaquer des cibles dans les pays de la CEI (Communauté des États Indépendants), respectant la ligne rouge de Moscou.
Conti / Trickbot	Ransomware (Conti), botnet (Trickbot), Vol de données. Institutions publiques occidentales.	Ces groupes ont manifesté un soutien public à la guerre en Ukraine, entraînant une fuite de données et une fragmentation, mais restant une menace majeure.
APT 28 / Fancy Bear	Institutions gouvernementales et diplomatiques occidentales via Cyber-espionnage, vol de données politiques et militaires, spear-phishing ciblé, exploitation zero day	Attribution largement établie au GRU (Russie), aligné sur les priorités géopolitiques russes et corrélées aux crises et échéances politiques
Sources : MITRE		

Sources : MITRE

Annexe C :

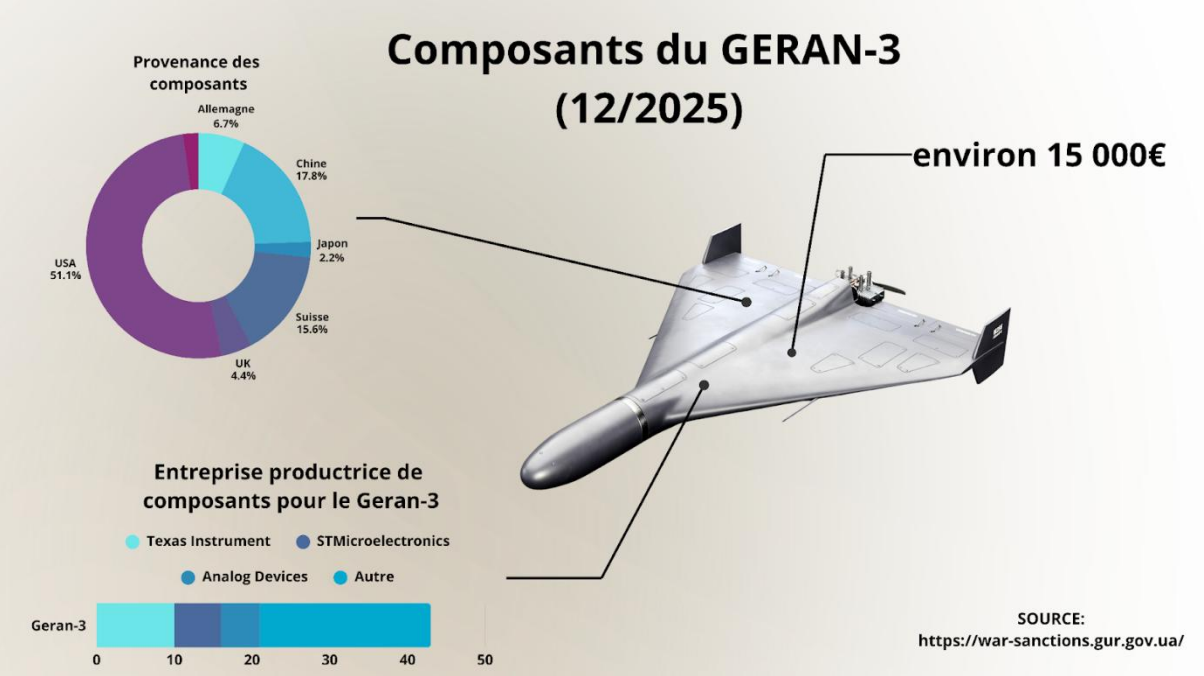
Entreprises cyber en Russie

Entreprise	Etat financier	Rôle stratégique	Lien avec l'état russe
Kaspersky	En 2024, performance robuste avec 11% de croissance tirée par les ventes B2B (+19% globalement), atteignant 822 millions USD. Les ventes B2C ont légèrement diminué (-2%) en raison des sanctions et de l'image de l'entreprise.	Approche défensive : L'entreprise fournit des logiciels antivirus (SIEM, XDR) pour points de terminaison destinés au secteur privé et à l'État	Eugene KasperskyPDG de l'entreprise en lien avec le KGB par sa formation. Soupçons de collaboration avec le FSB via la vente de trojan espion dans le antivirus.
Positive Technologies	Chiffre d'affaires : ~24,5 milliards de rubles (+10 % vs 2023)	Cybersécurité défensive : pentesting, audit, protection infrastructures critiques	Collaboration avec opérateurs stratégiques russes ; alignement sur la souveraineté numérique
Rostelecom Solar	Chiffre d'affaires 2025 : environ 12,8 milliards RUB, en hausse de ~16 % par rapport à l'année précédente.	Cybersécurité nationale : SOC, protection des administrations et infrastructures critiques	Filiale de Rostelecom, acteur clé dans la cybersécurité nationale et infrastructures critiques
InfoWatch	Chiffre d'affaires 2024 : 3,9 milliards de roubles (croissance de +50 % par rapport à 2023).	DLP (Data Loss Prevention), surveillance des flux d'information, protection contre les fuites internes	Présence dans les administrations et entreprises publiques, soutenue par fonds souverain et partenariats
RTSoft / Digital Security	N/A	Audit, pentesting, sécurité applicative ; intégré dans Solar (Rostelecom)	Intégré à Solar, aligné indirectement avec les priorités de souveraineté numérique et l'État

Sources : Verified Market

Sources : Verified Market

Annexe D:



Source : https://war-sanctions.gur.gov.ua/

6 Bibliographie :

Rapports

Atlantic Council. *Confronting Russia's Cyber Power*. Rapport stratégique. Atlantic Council – Digital Forensic Research Lab, 2025.

Centre for Naval Analyses (CNA). *Hacking and Firewalls Under Siege*. Rapport analytique. CNA, 2025.

Cybersecurity and Infrastructure Security Agency (CISA). *Russian State-Sponsored Cyber Threat Activity*. Alerte de cybersécurité AA25-343A. Département de la Sécurité intérieure des États-Unis, 2025.

Department of Health and Human Services (HHS). *Major Cyber Organizations of Russian Intelligence Services*. Rapport institutionnel. Gouvernement des États-Unis, 2023.

European Council on Foreign Relations (ECFR). *Putin's Hydra: Inside Russia's Intelligence Services*. Rapport stratégique. ECFR, 2024.

Government of Canada – Communications Security Establishment. *Cyber Threat Activity Associated with the Russian Invasion of Ukraine*. Rapport gouvernemental. Gouvernement du Canada, 2024.

Institut Delors. *The Cybersecurity Dimension of the War in Ukraine*. Policy Paper n°281. Institut Delors, 2025.

International Institute for Strategic Studies (IISS). *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*. Research Paper. IISS, 2025.

Ministère de la Défense de la République de Lituanie – National Cyber Security Centre (NCSC). *A Comparative Study of Russian Cyber Offensive Capabilities from 2022 to 2025*. Rapport ministériel. Gouvernement de Lituanie, 2025.

Organisation du Traité de l'Atlantique Nord (OTAN). *NATO Cyber Defence Report*. Rapport OTAN. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2021.

Recorded Future. *Dark Covenant 2: Cybercrime and the Russian State's War in Ukraine*. Rapport de renseignement cyber. Recorded Future Insikt Group, 2024.

Articles de journal

Bing, Christopher. « Noname057(16) hacking group targets Ukraine and allies ». *The Record*, 2024.
Disponible sur : https://therecord.media/noname-hacking-group-targets-ukraine-and-allies

Clément, Éric. « La Russie dans le cyberespace : Runet est-il le nouveau rideau de fer numérique ? ». *Portail de l'Intelligence Économique*, 2019.
Disponible sur : https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2019/la-russie-dans-le-cyberespace-runet-est-il-le-nouveau-rideau-de-fer-numerique/

Gallagher, Sean. « Un pirate informatique de légende à la tête du bras cyber du renseignement militaire russe ». *France 24*, 16 mars 2023.
Disponible sur : https://www.france24.com/fr/%C3%A9co-tech/20230316-un-pirate-informatique-de-l%C3%A9gende-%C3%A0-la-t%C3%AAte-du-bras-cyber-du-renseignement-militaire-russe

Henderson, James. « Russia ramps up cybersecurity systems ». *Jamestown Foundation*, 2023.
Disponible sur : https://jamestown.org/russia-ramps-up-cybersecurity-systems/

Koshkina, Olga. « German Gref : la transformation de Sberbank est un processus permanent ». *Forbes Russia*, 2024.
Disponible sur : https://www.forbes.ru/biznes/387895-german-gref-transformaciya-sberbanka-eto-vechnyy-process

Rault, Jean-Luc. « Supercalculateurs : la Russie veut être dans le top 10, mais cela semble improbable». *Futura Sciences*, 2024.
Disponible sur :https://www.futura-sciences.com/tech/actualites/informatique-supercalculateurs-russie-veut-etre-top-10-cela-semble-improbable-108351/

Rédaction NAE. « Le nouveau système anti-drone russe se fait détruire à cause d'un drone ». *Normandie AeroEspace*, 2024.
Disponible sur : https://www.nae.fr/le-nouveau-systeme-anti-drone-russe-se-fait-detruire-a-cause-dun-drone/

Schwarz, Oliver. « Intelligence artificielle et robotique : la stratégie russe ». *Xpert.Digital*, 2024.
Disponible sur : https://xpert.digital/fr/intelligence-artificielle-et-robotique-pour-la-russie/

Sharma, Rakesh. « Researchers uncovered how Russia leverages private companies in cyber operations ». *Cybersecurity News*, 2024.
Disponible sur :https://cybersecuritynews.com/researchers-uncovered-on-how-russia-leverages-private-companies/

Smirnov, Alexeï. « La Russie investit massivement dans les technologies quantiques ». *Trashbox.ru*, 12 août 2025.
Disponible sur : https://trashbox.ru/link/2025-08-12-rossiya-kvantovye-tehnologii

Articles de recherche

Badouard, R. *La désinformation russe à l'ère numérique*. in *EchoGéo*, n°56, 2021. Disponible sur : https://journals.openedition.org/echogeo/21804

Barichella, A. *The cybersecurity dimension of the war in Ukraine*. in *Policy Papers – Institut Delors*, n°281, 2025. Disponible sur : https://institutdelors.eu/content/uploads/2025/04/PP281_The-cybersecurity-dimension-of-the-war-in-Ukraine_Barichella_EN.pdf

Boulègue, M. *Un outsider paradoxal : la Russie dans la course à l'intelligence artificielle*. in *Institut français des relations internationales (IFRI)*, 2023. Disponible sur : https://www.ifri.org/fr/etudes/un-outsider-paradoxal-la-russie-dans-la-course-lintelligence-artificielle

Choucri, N., Madnick, S. *Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe*. in *ResearchGate*, 2024. Disponible sur : https://www.researchgate.net/publication/383846488_Cyberattacks_in_Russia's_hybrid_war_against_Ukraine_and_its_Ramifications_for_Europe

Defense Innovation and Emerging Technologies Office (DIEE). *Russian disinformation strategies and narratives*. Ministère de la Défense espagnol, 2025. Disponible sur: https://www.defensa.gob.es/documents/2073105/2320887/la_desinformacion_rusa_2025_dieeeo55_eng.pdf

E3S Conferences. *Digital transformation and cybersecurity strategies in Russia*. in *E3S Web of Conferences*, 2021. Disponible sur : https://www.e3s-conferences.org/articles/e3sconf/pdf/2021/72/e3sconf_esmgt2021_06013.pdf

Farkas, J., Bastos, M. *Russian information warfare: tactics, strategies and narratives*. in *Media and Communication*, Cogitatio Press, vol. 6, n°2, 2018. Disponible sur : https://www.cogitatiopress.com/mediaandcommunication/article/view/808

Sites web

Académie du Service fédéral de sécurité (FSB). *Présentation institutionnelle*. FSB de Russie, 2024. Disponible sur : http://academy.fsb.ru/index_i.html

Agence fédérale russe ONF. *Programme Kulibin – innovation militaire et civile*. ONF, 2024. Disponible sur : https://onf.ru/news/tags/kulibin

Gazprom Neft. *Digital Transformation Strategy 2030*. Gazprom Neft, 2018. Disponible sur : https://www.worldoil.com/news/2018/11/26/gazprom-neft-implements-2030-digital-transformation-strategy

NTechLab. *FindFace Multi – reconnaissance faciale*. NTechLab, 2024. Disponible sur : https://ntechlab.com/findface-multi/

Présidence de la Fédération de Russie. *Décrets et actes officiels*. Kremlin, 2023. Disponible sur : http://en.kremlin.ru/acts/news/73579

Présidence de la Fédération de Russie. *Discours et communiqués officiels du Président*. Kremlin, 2024. Disponible sur : http://en.kremlin.ru/events/president/news/77194

Telegram. *Ugolok_Sitha* [canal Telegram]. Source primaire russe, contenu consulté en 2024. Disponible sur : https://t.me/Ugolok_Sitha

U.S. Department of the Treasury. *Sanctions and enforcement actions related to Russia*. Trésor des États-Unis, 2024. Disponible sur : https://home.treasury.gov/news/press-releases/jy0127

Université technique nationale de Moscou (MPEI). *Centre militaire universitaire*. MPEI, 2024. Disponible sur : https://vuc.mpei.ru/Pages/default.aspx

Ecole de Guerre Economique

196 rue de Grenelle, 75007 Paris

ege.fr

AEGE – Le réseau d'experts en intelligence économique

aege.fr

portail-ie.fr

infoguerre.fr