Lettre mensuelle – Décembre 2019 – Disponible sur omc.ceis.eu

Table des matières

ANALYSES (1/2)

LA RUSSIE SE LANCE DANS LA COURSE À L'INTELLIGENCE ARTIFICIELLE

La Russie dispose d'un écosystème numérique propre et dense porté par de grandes entreprises comme Yandex ou Mail.ru, et entièrement régi par le droit russe. Constatant cependant que les développements dans le domaine de l'intelligence artificielle (IA) n'ont pas connu les mêmes succès qu'aux États-Unis ou en Chine[1], la nouvelle **Stratégie nationale pour le développement de l'intelligence artificielle[2]** russe ambitionne de renverser cette tendance pour faire de la Russie un véritable champion de l'IA.

Plus précisément, cette Stratégie vise à « *assurer le développement accéléré de l'IA dans la Fédération de Russie ainsi que la conduite de recherches scientifique dans le domaine de l'IA, l'amélioration de la disponibilité de l'information et des ressources informatiques* ». Elle se donne également pour objectif d' « *améliorer le bien-être et la qualité de vie de la population, assurer la sécurité nationale et l'État de droit* », ainsi que de garantir « *la compétitivité durable de l'économie russe* ».

Cette nouvelle Stratégie qui reflète l'ambition russe de venir concurrencer la Chine et les États-Unis dans le domaine de l'IA suppose cependant des adaptations organisationnelles, règlementaires et humaines qui pourraient ralentir sa mise en œuvre et ses effets. Ainsi, les dispositions envisagées par la Stratégie permettront sans doute plutôt à la Russie de rattraper un retard important en matière d'IA que de véritablement rivaliser ou dépasser les capacités et les innovations étrangères.

Une stratégie conçue pour concurrencer la Chine et les États-Unis…

Cette Stratégie prévoit d'abord de renforcer et consolider la base industrielle russe de l'IA, tant grâce à des investissements considérables, publics et privés, que par un soutien renouvelé à l'innovation, la R&D et la recherche scientifique. Ces efforts, toujours selon cette Stratégie, seront concentrés sur des secteurs et activités identifiés comme prioritaires, pour lesquels les besoins russes en matière d'IA sont les plus prégnants et les avantages attendus du développement des technologies de l'IA les plus significatifs. Au-delà de ces avantages non négligeables, le développement de l'IA à grande échelle et la multiplication des usages et applications basées sur ces technologies pourraient également être mis au profit de la cybersécurité et de la défense cyber de la Russie, qui s'est notamment fixée des objectifs ambitieux de robotisation des équipements militaires d'ici 2025.

[1] https://www.tresor.economie.gouv.fr/Articles/28619068-9771-411c-9a43-20fdaeb0adc8/files/5a885cf0-0af1-4243-be03-8857b5319fae

[2] http://static.kremlin.ru/media/events/files/ru/AH4x6HgKWANwVtMOfPDhcbRpvd1HCCsv.pdf

Renforcer et consolider l'écosystème industriel de l'IA

La Stratégie s'insère dans un corpus de textes avec lesquels il est prévu qu'elle soit mise en cohérence, comme le Programme national d'économie numérique (2019), la Stratégie pour le développement de la société informationnelle 2017-2030[3] (2017) et les projets de l'Initiative Nationale pour la Technologie (ITN) de 2015.

L'intelligence artificielle (IA) est en effet un véritable enjeu de puissance pour la Russie, comme le montrent de nombreux projets et initiatives nationaux auxquels cette nouvelle Stratégie donne un cadre. Une étude comparative des stratégies nationales en matière d'IA menée en 2017 en France par la DG Trésor du ministère de l'Économie et des Finances présente par exemple, parmi les nombreux projets russes en la matière, l'initiative Nationale pour la technologie (ITN). Portée par l'Agence pour les Initiatives Stratégiques (ASI), celle-ci prévoit la mise en place d'une série d'instruments de soutien à la R&D dans 9 marchés sur lesquels la Russie souhaite consolider sa position à l'horizon 2035 dont, sous le projet « Neuronet », les neuro-technologies, le *big data* et l'intelligence artificielle.

Moins connu que les solutions américaines ou chinoises, l'écosystème russe de l'innovation liée à l'IA n'en est pas moins riche, avec notamment les acteurs suivants[4] (liste non exhaustive) :

Principales applications de l'IA	Start-ups développant des solutions dans ces secteurs
Traitement du langage : lecture et analyse de texte non structuré, analyse des demandes des utilisateurs, traduction automatique, analyse de la tonalité et du contenu de texte, etc.	Eureka Engine Mivar
Analyse prédictive Prise de décision et prévision, publicité et personnalisation des propositions, scoring bancaire, optimisation des achats, prévision des propriétés des nouveaux matériaux et médicaments, médecine personnelle, optimisation des flux de transport, prévision de défaillance de l'équipement, *business intelligence*, etc.	Prognoz Aidata.me Data Mining Labs
Vision informatique : identification des visages et autres objets, analyse vidéo, description du contenu des images et des vidéos, reconnaissance de l'écriture manuscrite et des gestes, etc.	Prisma VisionLabs Cognitive Technologies
Technologies discursives : reconnaissance, analyse et synthèse du discours oral, biométrie vocale	Vocalize Speereo

[3] http://en.kremlin.ru/acts/news/54477

[4] https://www.tresor.economie.gouv.fr/Articles/28619068-9771-411c-9a43-20fdaeb0adc8/files/5a885cf0-0af1-4243-be03-8857b5319fae

Biométrie : voix, empreinte digitale, iris, ADN	NTechLab Vocalize BioSmart

Répondre à des enjeux industriels, économiques et sociaux

L'un des objectifs affichés de la Stratégie est de permettre aux technologies russes de se faire une place significative dans le marché mondial de l'IA. Elle dresse ainsi les **priorités** en termes de développement et d'applications de l'IA en Russie.

1) D'abord, l'IA doit contribuer à améliorer l'efficacité des entreprises en permettant des progrès dans les domaines suivants :

- **Prédiction et aide à la décision** : l'amélioration de la planification, de la prévision et des processus de prise de décision, incluant la maintenance prédictive et préventive, l'optimisation de la planification des approvisionnements et de la production et l'aide à la décision en matière de décision financière ;
- **Production industrielle** : l'automatisation des processus de production répétitifs ;
- **IoT** : l'utilisation d'équipements intelligents, de systèmes robotisés et de systèmes intelligents de gestion logistique ;
- **Sûreté et sécurité** : l'amélioration de la sécurité des employés, dont la prévention des risques et la réduction de la participation humaine aux processus présentant un risque élevé pour la santé, voire pour la vie ;
- **Expérience consommateur** : une plus grande satisfaction et fidélité des consommateurs, notamment grâce à des campagnes d'offres et de recommandations personnalisées ;
- **Ressources humaines** : l'optimisation de la sélection et de la formation du personnel, ainsi que l'optimisation de l'emploi du temps de chaque employé.

2) Dans la sphère sociale, l'IA doit faciliter la « *création de conditions favorisant l'amélioration du niveau de vie de la population* », grâce à des avancées attendues dans les domaines suivants :

- **Médical** : l'accroissement de la qualité des services médicaux (examens préventifs sur la base de l'analyse prédictive d'images, prédiction de l'évolution des maladies, sélection du dosage médicamenteux optimal, réduction des risques de pandémies, automatisation et précision des interventions chirurgicales…) ;
- **Enseignement** : l'amélioration de la qualité des services éducatifs (adaptation des processus d'apprentissage aux besoins des apprenants, optimisation de l'orientation professionnelle grâce à des indicateurs de performance et identification des enfants doués de capacités hors du commun, automatisation des processus d'évaluation, etc.)

- **Services publics** : l'amélioration de la qualité des services publics et municipaux ainsi que la réduction des coûts de mise en œuvre.

Par ailleurs, la Stratégie a aussi pour mission d'accroitre la participation d'organisations publiques et d'entreprises russes dans la recherche et le développement de solutions basées sur l'IA. Le nombre d'organisations et d'entités publiques qui utiliseront l'IA et qui participeront à son développement sera d'ailleurs utilisé comme indicateur du développement du marché de l'IA en Russie et donc des avancées de la Stratégie.

Des implications militaires et sécuritaires

Si la Stratégie d'IA concerne principalement le développement d'un écosystème d'IA propre à la Russie et s'adresse d'abord au monde de la recherche et des affaires, elle n'est pas sans avoir des implications pour la défense et la sécurité nationale.

En effet, la Stratégie d'IA doit être mise en perspective avec les objectifs fixés par l'état-major des forces russes de robotisation des équipements militaires d'ici à 2025 dans le but d'éviter d'exposer les soldats aux dangers du champ de bataille[5]. Dans ce cadre, la Stratégie relative à l'IA devrait servir de levier pour renforcer et accélérer les innovations dans les armées, notamment dans le développement de matériels et de systèmes d'armes autonomes[6].

Également, la Stratégie d'IA devrait être suivie de près par les services de renseignement russes comme le souligne le site Intelligence Online[7]. Directement impliqués dans la Commission gouvernementale au développement numérique qui est chargée de la coordination de la Stratégie, ils devraient s'intéresser particulièrement à deux aspects de la Stratégie d'IA concernant :

- le contrôle des algorithmes dans le but d'assurer la sécurité des applications russes d'IA et, inversement, pour détecter les risques d'utilisation malveillante de l'IA comme par exemple la diffusion automatique de fausses informations sur internet ou sur les réseaux sociaux ;
- les innovations d'IA dans le domaine des relations sociales afin de mieux détecter les mouvements sociaux pouvant causer des troubles à l'ordre public ou à la sécurité nationale.

Les orientations fixées par la Stratégie correspondent à la mise en place d'un écosystème de l'IA touchant l'ensemble de la vie économique et sociale du pays avec les bénéfices qui peuvent en résulter en matière de sécurité et de défense, ce qui n'est pas sans rappeler celui dont dispose les États-Unis avec les GAFAM ou encore la Chine avec les BATX. Néanmoins, si les mesures qui devraient être mise en œuvre permettront

[5] https://theconversation.com/la-strategie-russe-de-developpement-de-lintelligence-artificielle-127457 ; http://lignesdedefense.blogs.ouest-france.fr/media/00/00/3720123260.2.jpg ; http://www.slate.fr/story/149961/robots-armes-autonomes

[6] https://www.rt.com/news/414107-putin-military-ai-hint/

[7] https://www.intelligenceonline.fr/diplomatie-parallele/2019/10/16/les-services-de-renseignement-du-kremlin-fondent-sur-l-ia,108377315-art

sans doute à la Russie de rattraper son retard en matière d'IA, il est peu probable en revanche qu'elle lui permette de dépasser ses concurrents.

… Mais qui permettra sans doute juste à la Russie de rattraper son retard

Les mesures envisagées pour mettre en œuvre les orientations de la Stratégie Russe d'IA sont de 3 types :

- l'amélioration de la connaissance en matière d'IA, en renforçant le soutien à la recherche scientifique et en s'ouvrant à l'international ;
- des efforts en matière d'investissements financiers publics et privés ;
- des efforts en matière de réglementation.

Ces mesures visent principalement à permettre aux chercheurs et entreprises russes de se mettre rapidement et plus facilement à niveau sur des avancées actuelle de l'IA dans le monde et dans les différents secteurs d'activité.

Un soutien accru à la recherche scientifique et une ouverture à l'international

Le soutien à la recherche scientifique est présenté comme la pierre angulaire de la Stratégie et sera financé par des mécanismes de financement existants. La recherche sera essentiellement orientée vers la simulation algorithmique de systèmes de prise de décision inspirés de systèmes biologiques, vers l'apprentissage automatique et le développement d'algorithmes adaptatifs, ainsi que vers la décomposition automatique des processus.

L'accent est également mis sur l'ouverture à l'international[8]. La Stratégie promeut les échanges de spécialistes et la participation d'experts russes à de grandes conférences internationales. D'ici 2024, le principal indicateur de la bonne mise en œuvre de mesures de soutien à la recherche sera l'accroissement du nombre d'articles de spécialistes russes de l'IA publiés dans de grandes revues scientifiques internationales, du nombre d'entités et d'entreprises enregistrées ayant une activité dans le domaine de l'IA, et du nombre de solutions basées sur l'IA réellement mises en œuvre. La façon dont ces solutions seront recensées n'est toutefois pas précisée. En outre, l'ouverture à l'international consiste à :

- permettre aux entreprises et aux universités russes de s'investir davantage dans des forums internationaux ou des projets internationaux comme par exemple des compétitions technologiques pour stimuler l'innovation (Olympiade de l'informatique[9] ou l'International Collegiate Programming Contest[10] par exemple) ;

[8] https://theconversation.com/la-strategie-russe-de-developpement-de-lintelligence-artificielle-127457
[9] https://ioinformatics.org/
[10] https://icpc.baylor.edu/

- recruter davantage d'experts nationaux et étrangers qui bénéficieront d'un salaire et de conditions de travail attractifs comme par exemple la possibilité de télétravail ou la garantie du respect des procédures relatives à l'obtention de la citoyenneté russe et des permis de travail.

Ces mesures devraient notamment servir à lutter contre « la fuite massive des cerveaux » vers les États-Unis ou l'Europe et pourraient permettre aux entreprises et universités russes de pallier leurs difficultés pour obtenir des données nécessaires pour le développement de l'IA[11].

Des efforts relatifs en matière d'investissement

Si la Stratégie reste muette sur les investissements à prévoir pour le développement de l'IA, la participation d'investisseurs privés russes dans des startups de l'IA semble en augmentation depuis 2016. A titre d'exemple, les sociétés d'investissements Larnabel VC et VP Capitals ont créé un fonds de 100 millions de dollars pour le développement de startups d'IA tout secteur confondu[12]. En outre, la première banque de Russie, Sberbank, très active dans le développement de l'écosystème numérique russe avec Yandex[13], devrait également être amenée à jouer un rôle important dans les investissements liés à l'application de la Stratégie[14]. Par ailleurs, la Russie semble coopérer en matière d'IA avec des investisseurs venant d'Asie et du Moyen-Orient. Le fonds souverain russe (RDIF) et le fonds saoudien (PIF) ont ainsi annoncé avoir signé des accords pour un montant global de 2 milliards de dollars et portant notamment sur l'IA[15]. Néanmoins, les capacités d'investissement de la Russie peuvent paraitre encore très limitées en comparaison de celles des États-Unis[16].

Des adaptations réglementaires et législatives

La Stratégie souligne la nécessité d'adapter la réglementation relatives aux interactions humaines, ainsi que la formulation de normes éthiques. Il est toutefois précisé qu'une réglementation excessive pourrait ralentir considérablement le développement et l'introduction de solutions technologiques. Cette réglementation passera entre autres par des « *conditions légales favorables pour l'accès aux données anonymisées, notamment collectées par des autorités publiques et des organisations médicales* » et la mise en œuvre de

[11] Selon le rapport de la DG Trésor de 2017, les entreprises et universités russes sont confrontés à plusieurs difficultés sur le marché de l'IA, notamment : « *le caractère fermé des entreprises russes rend difficile l'obtention des données nécessaires au développement de l'IA* » et « *l'intégration faible de la Russie dans les échanges internationaux de données et dans la coopération universitaire* ».

[12] https://venturebeat.com/2017/03/27/a-new-100-million-russian-investment-fund-is-targeting-ai-startups-globally/

[13] https://www.lesechos.fr/finance-marches/banque-assurances/sberbank-lex-banque-sovietique-qui-mise-sur-le-digital-1036379

[14] https://www.frenchweb.fr/la-russie-se-lance-dans-la-course-a-lintelligence-artificielle/379401 ; https://www.tresor.economie.gouv.fr/Articles/28619068-9771-411c-9a43-20fdaeb0adc8/files/5a885cf0-0af1-4243-be03-8857b5319fae

[15] https://www.lesechos.fr/monde/afrique-moyen-orient/la-russie-et-larabie-saoudite-scellent-leur-rapprochement-1139922

[16] https://www.rt.com/news/414107-putin-military-ai-hint/

« *conditions d'accès aux données, incluant les données personnelles, pour la recherche scientifique et la création de technologies d'IA* ».

Au regard des importants efforts administratifs et réglementaires, organisationnels, humains et d'investissements qu'implique la mise en œuvre de cette nouvelle Stratégie, il n'est donc pas certain que la Russie puisse réellement disposer d'un écosystème d'IA indépendant qui puisse concurrencer celui des États-Unis ou de la Chine d'ici 2030. De plus, la Russie fera face à une limite intrinsèque relative aux quantités de données qu'elle est théoriquement en capacité de collecter puis d'exploiter : sa démographie. Si la Russie compte aujourd'hui plus de 144 millions d'habitants, la Chine, avec ses 1,39 milliard d'habitants, a accès à un nombre de données monumental permettant d'alimenter ses algorithmes d'intelligence artificielle. A titre d'exemple, les géants chinois Baidu, Alibaba et Tencent disposeraient en effet « *de plus de données que les Etats-Unis et l'Europe réunis* »[17]. La démographie russe, en baisse depuis quelques années, pourrait donc freiner les ambitions politiques en matière d'IA, mais pourraient également en partie expliquer la volonté d'ouverture à l'internationale. Les capacités réelles de financement de la Stratégie posent également question. Très peu d'éléments sont en effet donnés quant aux sources de financement de la Stratégie. Néanmoins, l'échéance de 2024, dont le choix n'est pas explicité, pourrait servir de date intermédiaire permettant d'évaluer, presque à mi-parcours, la capacité de la Russie à rattraper son retard en matière d'IA, et si besoin ajuster les mesures et dispositifs prévus par cette Stratégie pour atteindre ces objectifs.

[17] https://www.lemondeinformatique.fr/actualites/lire-intelligence-artificielle-quand-la-chine-aura-pris-le-pouvoir-73417.html

ANALYSES (2/2)

L'AFFAIRE « ALEKSEI BURKOV » : UN PRÉSUMÉ CYBERCRIMINEL AU CŒUR D'UN BRAS DE FER DIPLOMATIQUE

Sur demande d'Interpol, le ressortissant russe Aleksei Burkov a été arrêté en décembre 2015 à l'aéroport Ben Gourion de Tel-Aviv, accusé de fraude électronique, intrusion informatique, vol d'identité et blanchiment d'argent. Face aux États-Unis qui demandaient son extradition, pour qu'il puisse être jugé par les autorités américaines, Moscou s'est engagé dans une véritable bataille diplomatique pour obtenir le rapatriement du présumé pirate informatique, alimentant des rumeurs sur ses supposés liens avec le gouvernement russe[18]. Finalement extradé vers Washington, Burkov a comparu pour la première fois le 12 novembre 2019 devant le tribunal fédéral du district oriental de Virginie. Loin d'être un cas isolé, son affaire reflète bien l'enjeu que constitue, pour la Russie comme pour les États-Unis, l'arrestation de pirates informatiques russes, dans un contexte de confusion croissante entre les activités de « cybercriminalité » et de « cyberespionnage ».

1. Retour sur l'affaire Aleksei Burkov

Aleksei Burkov : un hacker d'élite aux activités ambiguës ?

Selon son acte d'accusation[19], Burkov est suspecté d'avoir alimenté deux forums russophones sur le Darknet, respectivement consacrés à la fraude à la carte bancaire et au piratage informatique. Il est notamment accusé d'avoir été à la tête de CardPlanet, une plateforme dédiée à la vente de numéros de cartes de paiement, aujourd'hui désactivée, et qui reposait sur une base de données de plus de 150 000 cartes compromises. Leur majorité aurait été délivrée par une entité bancaire enregistrée dans le district oriental de l'État de Virginie. Obtenus via des intrusions informatiques, les numéros de ces cartes auraient permis des achats frauduleux d'une valeur totale, pour les seules cartes américaines, estimée à 20 millions USD.

Le nom du second forum n'a pas été rendu public afin de ne pas compromettre l'enquête en cours[20]. L'acte d'accusation évoque une plateforme où les « cybercriminels d'élite » pouvaient planifier des attaques, acheter et/ou vendre des biens et services (données personnelles, logiciels malveillants, etc.). Il met également en lumière le caractère très exclusif de ce forum qui était régi par des conditions restrictives : chaque adhérent devait être parrainé par trois membres et s'acquitter d'une caution pouvant s'élever jusqu'à 5 000 USD.

D'après les investigations conduites par *KrebsOnSecurity*, Burkov aurait aussi opéré sur d'autres forums russophones sous le pseudonyme de « K0pa », qui est le surnom de l'un des administrateurs des plateformes

[18] Bar Peleg, Josh Breiner, « Russian Hacker Jailed in Israel Says He's Not a Spy, Denies Meddling in U.S. Election », *Haaretz* [en ligne], 3 novembre 2019.
[19] « Russian National Extradited for Running Online Criminal Marketplace », *US DoJ* [en ligne], 12 novembre 2019.
[20] Jeff Stone, « Aleksei Burkov, Russian accused of operating 'elite' hacking forum, pleads not guilty », *Cyber Scoop* [en ligne], 22 novembre 2019.

Mazafaka et *DirectConnection*. Les conditions d'accès de ces dernières auraient été similaires à celles établies dans l'acte d'accusation. En remontant l'adresse courriel qu'il utilisait, *KrebsOnSecurity*, a pu établir que le même K0pa aurait également joué un rôle clé sur les forums *Spamdot* et *Verified*, en plus d'avoir été un membre-fondateur des « CyberLords ». Pendant près d'une décennie, ce groupe de hackers a publié en ligne des outils de piratage et des exploits ciblant des vulnérabilités longtemps inconnues[21].

Selon un ancien responsable américain[22], le second forum sur lequel Burkov aurait été actif et pour lequel il est inculpé ne correspondrait ni à *Mazafaka*, ni à *DirectConnection*. Alors que ses liens avec l'un de ces forums restent à être prouvés, la justice américaine reste convaincue que Burkov est bien lié à la cybercriminalité russe. Andrei Klimov, représentant du comité pour les Affaires internationales du Conseil de la fédération de Russie, a admis qu'il était possible que Burkov possède « certaines informations », ce qui expliquerait les accusations américaines[23].

Aleksei Burkov : la partie immergée de l'iceberg ?

Loin d'être un cas isolé, l'affaire Burkov fait écho à d'autres cas d'arrestations de présumés cybercriminels russes par la justice américaine. Comme Burkov, ces derniers sont de supposés cybercriminels dont les années de naissance oscillent entre 1980 et 1990. Ils représentent cette génération qui a connu directement l'effondrement de l'URSS, une économie sinistrée, la paupérisation de la population et d'importantes inflations. Ce contexte socio-économique pourrait expliquer le tropisme de cette classe d'âge pour le piratage informatique comme source de revenus, favorisé par une législation floue sur les questions cybernétiques.

Hackers russes extradés vers les États-Unis[2425262728]

Nom	Naissance	Faits reprochés	Arrestation	Date d'extradition	État
Aleksei Burkov	1989 1990	Animation de forums liés à la fraude à la CB et à la cybercriminalité	Israël Décembre 2015	Novembre 2019	Première comparution (Novembre 2019)
Andrei Tyurin	1984 1985	Intrusions massives dans des institutions financières	Grèce 2017		En attente d'extradition vers la France

[21] « Why Were the Russians So Set Against This Hacker Being Extradited? », *KrebsonSecurity* [en ligne], 18 novembre 2019.
[22] *Op. cit.* Jeff Stone, *Cyber Scoop* [en ligne], 22 novembre 2019.
[23] *Op. cit.* Natalya Bashlykova, *Izvestia* [en ligne], 18 novembre 2019 (en Russe).
[24] « Yevgeniy Nikulin Appears In U.S. Court Following Extradition », *US DoJ* [en ligne], 30 mars 2018.
[25] « United States vs. Peter Levashov », *US DoJ* [en ligne], 20 décembre 2018.
[26] « Russian cybcercriminal Roman Seleznev pleads guilty in Atlanta », *US DoJ* [en ligne], 8 septembre 2017.
[27] « Les États-Unis condamnent Martyshev pour cyber-fraude », *RT* [en ligne], 19 avril 2019 (en Russe).
[28] « Russian Hacker Who Used Neverquest Malware To Steal Money From Victims' Bank Accounts Pleads Guilty In Manhattan Federal Court », *US DoJ* [en ligne], 22 février 2019.

Yevgeniy Nikulin	1986 1987	Compromission de millions de mots de passe (LinkedIn, Dropbox et Formspring)	Rép. Tchèque Octobre 2016	Mars 2018	Procès en cours
Peter Levashov	1979 1980	Spamming/vol de bitcoins via des botnets, et animation de forums de cybercriminalité	Espagne Avril 2017	Février 2018	Procès en cours
Yury Martyshev	1982 1983	Développement d'un service de test de malwares avant leur mise en oeuvre	Lettonie Avril 2017	Juin 2017	Condamnation à 6,5 mois de prison (Avril 2019)
Stanislav Lisov	1985 1986	Création du cheval de Troie « NeverQuest » à l'origine de pertes estimées à des millions USD	Espagne Janvier 2017	Janvier 2018	Condamnation à 4 ans de prison (Février 2019)
Roman Seleznev	1984 1985	Vol de données de cartes de crédit qui a suscité la perte de millions de dollars	Maldives 2014	2014	Condamnation à 27 ans de prison (Avril 2017)

Burkov fait partie des quelques pirates informatiques russes à avoir été extradés vers les États-Unis. Une comparaison d'ensemble montre que les faits reprochés sont liés à de la cybercriminalité classique, allant de la fraude à la carte bancaire au vol de données personnelles, en passant par l'animation de forums. Les chefs d'inculpation sont similaires (fraude électronique, intrusion informatique, dommage intentionnel sur un ordinateur protégé, vol aggravé d'identité, blanchiment d'argent, complot).

La différence majeure réside toutefois dans la durée qui sépare les arrestations et extraditions. Pour Burkov, cet intervalle est de quatre ans, alors qu'il ne dépasse pas – en attendant l'extradition d'Andrei Tyurin – les deux dans les autres cas. Ce délai pourrait s'expliquer par l'implication plus intense de Moscou dans ce dossier que dans les précédents. La pression exercée par la Russie pour obtenir son rapatriement afin qu'il soit appréhendé par la justice nationale est assez inhabituelle[29]. Outre des échanges politiques de haut niveau avec Tel-Aviv[30], plusieurs demandes de voie de recours ont été formulées auprès des plus hautes juridictions israéliennes. Les autorités russes auraient également arrêté une citoyenne israélo-américaine en avril 2019 pour « détention de stupéfiants », dans la perspective potentielle d'un échange de prisonniers[31]. Infructueux, les efforts russes laissent toutefois penser que la réalité des activités de Burkov est telle que le Kremlin ne peut se permettre de le laisser à la justice américaine. Plus largement, cette bataille diplomatique reflète bien les efforts de plus en plus manifestes de la Russie pour empêcher l'extradition de ses présumés cybercriminels, plus particulièrement vers les États-Unis[32].

Les arrestations et inculpations de ressortissants russes aux États-Unis et à l'étranger se sont en effet accrues ces dernières années, dans le contexte de soupçons d'ingérence russe dans les élections présidentielles américaines de 2016. Avec une moyenne de deux par an pour la période 2010-2016, leur nombre s'est élevé

[29] Josh Breiner, Bar Peleg, Lisa Rozovsky, « No Kremlin Link Found to Russian Hacker Awaiting Extradition in Israel, Lead Investigator Says », *Haaretz* [en ligne], 17 octobre 2019.
[30] Tova Tzimuki, « Israel sets to extradite Russian hacker to U.S. », *Ynet News* [en ligne], 14 octobre 2019.
[31] *Op. cit.* Jeff Stone, *Cyber Scoop* [en ligne], 22 novembre 2019.
[32] Dustin Volz, Felicia Schwartz, « Moscou ne recule devant rien pour éviter à ses hackers une extradition vers les Etats-Unis », *L'Opinion* [en ligne], 6 novembre 2019.

à sept en 2017[33] dont quatre pour des faits de cybercriminalité (cf. tableau précédent). En novembre 2018, la Russie a accusé les États-Unis de « chasser » et « d'enlever » ses citoyens dans le monde, recommandant même à sa population de limiter ses déplacements à l'étranger[34]. En l'absence d'accord bilatéral en la matière, la stratégie américaine pour obtenir l'extradition de cybercriminels repose sur l'arrestation de suspects lorsqu'ils quittent la protection juridique de la Fédération de Russie en se rendant dans un État-tiers.

La Fédération de Russie s'efforce de son côté de protéger ses ressortissants dont l'extradition est interdite par l'article 61 de sa Constitution. Ce cadre politique et juridique pourrait expliquer la diversité des moyens techniques mises en œuvre pour rapatrier les citoyens inquiétés par des justices étrangères. À cet égard, certains responsables américains dénoncent des méthodes coercitives telles que la corruption, ainsi que des tentatives d'exploiter le système juridique, visant à faire pression sur les pays-tiers afin qu'ils bloquent les demandes d'extradition formulées par les États-Unis[35].

Dans ce contexte, la forte implication de Moscou pour éviter l'extradition de Burkov pourrait constituer une réponse aux efforts répétés de la justice américaine d'arrêter et de faire extrader des cybercriminels, sans forcément supposer de liens avec le Kremlin. Les efforts de la diplomatie russe ne pourraient toutefois être entièrement anodins non plus. Les États-Unis présument une grande influence de Burkov sur la cybercriminalité russe, faisant de lui une potentielle source d'informations sur le fonctionnement de cet écosystème. Dans le cas où les faits d'inculpation s'avèrent, obtenir son rapatriement aurait constitué une opportunité pour les autorités russes de l'enrôler en vue d'exploiter son expertise technique.

2. De la cybercriminalité à l'espionnage

Des cybercriminels russes accusés d'espionnage

L'affaire Burkov laisse supposer des activités qui dépassent le cadre de la cybercriminalité pour celui du cyberespionnage, voire plus largement une certaine connivence entre les services de renseignement et les cybercriminels russes. Dans le contexte des efforts de la Russie pour protéger sa souveraineté dans le cyberespace, de telles interactions seraient en effet envisageables. Les États-Unis soupçonnent d'ailleurs certains d'entre eux d'entretenir des relations avec les Forces armées de la Fédération de Russie (RuAF) :

[33] Polina Ivanova, « Russia says U.S. 'hunting' for Russians to arrest around the world », *Reuters* [en ligne], 2 février 2018.
[34] Tom Balmforth, « Moscow accuses U.S. of hunting Russians after Israel extradites suspected hacker », *Reuters* [en ligne], 13 novembre 2018.
[35] *Op. cit.* Dustin Volz, Felicia Schwartz, *L'Opinion* [en ligne], 6 novembre 2019.

Cybercriminels russes appartenant ou soupçonnés de liens avec les RuAF[3637383940]

Identité	Naissance	Faits reprochés	État
Maksim Yakubets	1987	Malware Bugat/Cridex/Dridex : - vol des identifiants de centaines de banques et institutions financières dans plus 40 pays ; - pertes de centaines de millions USD dep. 2011.	Recherchés par le FBI depuis décembre 2019
Evgeniy Bogachev	1983	Créateur du malware "GameOver Zeus" (GOZ) : - plus d'un million d'infections informatiques ; - pertes financières de plus de 100 millions USD.	Recherché par le FBI depuis mars 2017
Agents des services de renseignements			
Sept officiers du GRU		Cyberattaques sur des agences antidopage et instances sportives internationales	Recherchés par le FBI depuis octobre 2018
Douze officiers du FSB		Ingérence dans les élections de 2016 Vol de données du Comité national démocrate	Recherchés par le FBI depuis juillet 2018
Deux officiers du FSB		Vol de données de 500M utilisateurs de Yahoo	Recherchés par le FBI depuis mars 2017

La majorité des pirates informatiques russes accusés de cyberespionnage sont des officiers issus du Service fédéral de sécurité de la Fédération de Russie (FSB) et de la Direction générale des renseignements (GRU). Peu de civils sont soupçonnés de faits d'espionnage, exceptés Maksim Yakubets et Evgeniy Bogachev, dont les accusations officielles se limitent à des pertes financières liées au développement et à l'exploitation de logiciels malveillants. L'hypothèse que ces outils ont pu être utilisés par les RuAF dans le cadre d'activités de cyber renseignement peut en revanche être émise. Contrairement au cas de Yakubets, l'acte d'accusation contre Burkov n'établit aucune suspicion de relations avec les RuAF.

La cybercriminalité au service du renseignement ?

La nomination en 2012 du général d'armée Sergueï Choïgou à la tête du ministère de la Défense s'est traduite par une implication plus importante des militaires dans les affaires cybernétiques. Son arrivée coïncide avec l'acception d'une thèse selon laquelle la Russie serait victime d'une « guerre de l'information » au niveau mondial. Ce nouveau paradigme expliquerait la stratégie du Kremlin de former et d'encourager la formation de pirates informatiques afin de conduire des activités de cyberespionnage.

---

[36] « Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware », *US Department of the Treasury* [en ligne], 5 décembre 2019.

[37] « Actions in Response to Russian Malicious Cyber Activity and Harassment », *Obama White House* (Archives) [en ligne], 29 décembre 2016.

[38] « U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations », *US DoJ* [en ligne], 4 octobre 2018.

[39] « Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election », *US DoJ* [en ligne], 13 juillet 2019.

[40] « U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts », *US DoJ* [en ligne], 15 mars 2017.

Les RuAF auraient rapidement envisagé de recruter des cybercriminels. Dans un article intitulé *Enlisted Hacker* publié dans le journal gouvernemental Rossiiskaya Gazeta (2013), l'ancien vice-ministre de la Défense, le général de corps d'armée Oleg Ostapenko, a déclaré que les « escadrons scientifiques » (unités de cyberdéfense composées de civil établies dans plusieurs bases militaires du pays[41]) pouvaient faire l'objet d'un élargissement vers des pirates informatiques ayant des antécédents criminels, dans le but d'exploiter leurs capacités techniques. Un tel choix stratégique pourrait déboucher sur de potentielles coopérations entre les autorités russes et certains cybercriminels incarcérés en échange de leur libération[42].

Répondant aux soupçons d'ingérence dans les élections américaines de 2016, Vladimir Poutine a indiqué que les suspects étaient des « gens libres », « artistes » et « patriotes »[43]. Autrement dit, tant que les cybercriminels ne vont pas à l'encontre des intérêts nationaux, il n'est pas nécessaire de les surveiller de près ou de les recruter. La stratégie russe consisterait ainsi à laisser se former des groupes et des pirates informatiques isolés, plus ou moins autonomes, qui auront besoin un jour ou l'autre d'une protection de l'État ou dont les autorités pourraient avoir besoin. Figurant parmi les cybercriminels les plus recherchés au monde, Bogachev aurait permis au Kremlin de collecter des informations classifiées en Turquie et en Ukraine[44].

Les accusations de cyberespionnage, un moyen de pression politique ?

Les précédents exemples mettent en exergue une tendance globale des États-Unis à poursuivre des ressortissants d'autres pays, qu'ils soient hackers, espions ou les deux. Outre la Russie, avec le cas de Yakubets qui aurait contribué « aux efforts malveillants du gouvernement russe en matière cyber[45] », la Chine est aussi particulièrement visée. Il est par ailleurs intéressant de noter que Moscou et Pékin ne contestent pas spécialement le cyberespionnage des États-Unis et n'ont jamais accusé directement des citoyens américains des mêmes faits. Les pirates informatiques chinois recherchés par le FBI le sont principalement pour des faits de vol de propriété industrielle, dans un contexte où les États-Unis accusent la Chine de cyberespionnage au profit de ses progrès technologiques, sa modernisation militaire et ses objectifs économiques[46].

[41] A. Kramer, « How Russia recruited elite hackers for its cyberwar », *The New York Times* [en ligne], 29 décembre 2016.
[42] *Ibid*.
[43] « Maybe Private Russian Hackers Meddled in Election, Putin Says », *The New York Times* [en ligne], 1er juillet 2017.
[44] Op. cit. *KrebsOnSecurity*, 18 novembre 2019.
[45] *Op. cit. US Department of the Treasury* [en ligne], 5 décembre 2019.
[46] *Foreing Economic Espionage in Cyberspace*, NCSC, Director of National Intelligence, 24 juillet 2018, p. 5.

Hackers chinois recherchés par les États-Unis[47][48][49][50]

Identité	Motifs d'inculpation	État
Fujie Wang	Campagnes d'intrusion ciblant les systèmes informatiques de grandes entreprises aux États-Unis (dont une grande société de prestations de santé dans l'Indiana).	Recherché par le FBI depuis mai 2019
Zhu Hua	Campagnes d'intrusions mondiales dans les systèmes informatiques visant à voler des données, la propriété intellectuelle et des informations commerciales et technologiques confidentielles d'au moins 45 entreprises commerciales et de défense.	Recherché par le FBI depuis décembre 2018
Zhang Shilong		
5 officiers de l'Armée populaire de Libération	Piratage informatique, espionnage économique et autres infractions dirigées contre six entreprises américaines (notamment des industries de l'énergie nucléaire et métallurgiques).	Recherché par le FBI depuis mai 2014

En pleine guerre commerciale entre la Chine et les États-Unis, les accusations contre Fujie Wang (2019), Zhu Hua et Zhang Shilong (2018) revêtent une signification singulière. À l'instar de la Russie, la Chine n'extrade pas ses ressortissants et aucun traité en la matière ne la lie aux États-Unis. Au regard des difficultés d'attribution, les accusations de cyberespionnage contre des ressortissants chinois constitueraient davantage un moyen de montrer à l'échelle internationale que la Chine n'est pas un partenaire loyal. Dans une autre mesure, elles permettraient de mettre Pékin en porte-à-faux sur ses engagements relatifs à son accord de cybersécurité avec Washington, qui visait à réduire l'espionnage économique entre les deux pays (2015).

Contrairement à la cybercriminalité, le cyberespionnage ne fait pas l'objet de réglementation. Son encadrement relève de l'espionnage, réprimandé par les législations nationales mais qui n'est ni autorisé, ni prohibé par le droit international. Il est néanmoins admis qu'un acte d'espionnage peut constituer un fait internationalement illicite[51]. Par ailleurs, si le droit des conflits armés (notamment l'article 24 de la convention de La Haye) reconnaît un statut à l'espion en temps de guerre, ce dernier peut difficilement s'appliquer dans le cyberespace. Le cyberespionnage ne requiert en effet pas l'envoi physique d'agents et les États reconnaissent le cyber comme un domaine et non comme un territoire. Pour certains pays, il est davantage considéré comme un acte « inamical » voire « inacceptable » (Allemagne, États-Unis, France, etc.). Le cyberespionnage étant devenue une activité essentielle pour la protection de la sécurité nationale[52], les États se satisfont de cette « zone grise ».

Face à des extraditions finalement peu nombreuses, la stratégie américaine montre qu'elle n'est pas toujours utile au plan judiciaire mais qu'elle constitue davantage un moyen de pression politique. Le cyberespionnage

[47] Zhu Hua, *FBI* [en ligne], 20 décembre 2018.
[48] Zhang Shilong, *FBI* [en ligne], 20 décembre 2018.
[49] Fujie Wang, *FBI* [en ligne], 7 mai 2019.
[50] « Five Chinese Military Hackers Charged », *FBI* [en ligne], 19 mai 2014.
[51] Par exemple, les opérations d'un drone de surveillance peuvent violer la souveraineté d'un État survolé.
[52] « Le cyber-espionnage en droit international », *France Culture* [en ligne], 13 juin 2016 (Audio).

fait partie des arguments mis en avant pour accuser certains pirates informatiques. Néanmoins, contrairement à la cybercriminalité qui a fait l'objet d'un encadrement juridique avec la Convention de Budapest, le cyberespionnage est « toléré » dans le droit international. Son utilisation accrue dans des motifs d'inculpation tend à nourrir une certaine confusion avec la cybercriminalité.

FOCUS INNOVATION

Olvid, une messagerie instantanée sécurisée

Présentation

Olvid, créée en mai 2019, est le fruit de 5 années de R&D de 4 experts en cryptographie.

Le projet était, depuis 2017, hebergé par l'incubateur Agoranov co-fondé par l'ENS, Paristech, l'Université Paris Dauphine, la Sorbonne et l'Inria avant de rejoindre l'accélérateur Wilco en mars 2019, et d'intégrer le programme d'accélération Shake'Up de Wavestone en septembre 2019

L'innovation

Olvid apporte une réponse aux messageries instantanées grand public comme WhatsApp mais aussi Telegram ou Signal, qui obligent les utilisateurs à faire confiance à leur propre serveur sans garantie aucune sur leur sécurité. Ces solutions de messagerie font donc courir à leurs utilisateurs des risques multiples allant du déchiffrement des échanges à la manipulation des identités, en passant par l'exploitation des données personnelles, ou encore le risque d'exploitation par des acteurs malveillants voire même l'espionnage par des acteurs étatiques ou industriels.

Contrairement aux autres solutions de communication, la solution proposée par Olvid ne s'appuie pas sur un annuaire centralisé et ne fait plus reposer la sécurité des communications sur des serveurs.

Le serveur d'Olvid ne sert en effet qu'à assurer la distribution des messages, c'est par lui que transitent les clés de chiffrement (clés publiques) ainsi que les échanges chiffrés. Il est herbergé dans un cloud sur un infrastructure 100% « serverless » dont les data centers sont situés à Paris et Franckfort.

La technologie

La solution d'authentification HIAsecure permet de

- Sécuriser une authentification, en s'assurant que c'est bien la personne qui possède la convention qui est authentifiée ;
- De réduire les risques d'une authentification frauduleuse sur un service grâce à une solution d'authentification mouvante et donc extrêmement difficile à résoudre par un attaquant et/ou une intelligence artificielle ;

- De compléter une solution d'authentification déjà existante (biométrie, mot de passe/login, etc.).

Pour garantir la sécurité totale et définitive des échanges, Olvid propose un modèle de sécurité qui repose sur des protocoles cryptographiques permettant de prouver mathématiquement l'intégrité, la confidentialité et l'anonymat des communications grâce à un chiffrement *end-to-end*.

La solution d'Olvid répond donc à 3 exigences de la sécurité des échanges qui ne sont réunies dans aucune autre solution de communication :

- L'authentification des utilisateurs - avec notamment l'établissement d'un canal sécurisé entre 2 utilisateurs via l'échange d'un code à 4 chiffres ;
- Le chiffrement des échanges ;
- Le chiffrement des métadonnées.

Elle permet donc de garantir, même en cas de compromission du serveur :

- La confidentialité des échanges ;
- L'anonymat des interlocuteurs.

L'architecture du cœur cryptographique d'Olvid a été conçue pour prendre en compte l'impact potentiel des futurs ordinateurs quantiques en termes de résistance des algorithmes cryptographiques. La cryptographique à clé secrète sur laquelle repose cette solution est ainsi déjà résistante à ces nouveaux ordinateurs, contrairement aux primitives à clé en l'absence de standard « post-quantique » reconnu.

CALENDRIER

28-30/01/2020 (LILLE)
FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ (FIC2020)

Co-organisé par la Gendarmerie nationale et CEIS, avec le soutien de la Région Hauts-de-France, le FIC est devenu l'événement européen de référence en matière de sécurité et de confiance numérique. Il représente un moment privilégié de réflexion stratégique entre les acteurs publics et privés impliqués, qui continuent d'y jouer un rôle essentiel.

La prochaine édition se tiendra à Lille Grand Palais du 28 au 30 janvier 2020 sur le thème « Replacer l'humain au cœur de la cybersécurité ».

Et si les utilisateurs n'étaient pas seulement une menace, mais plutôt l'une des réponses aux défis posés par la cybersécurité ? À l'opposé des architectures zero trust basées sur la "méfiance par défaut", il serait sans

doute plus efficace -et moins onéreux- de redonner à l'utilisateur une place centrale en faisant de lui un véritable acteur de la cybersécurité de son organisation. Une telle approche nécessiterait cependant non seulement de repenser les interactions homme-machine pour rendre la sécurité plus intuitive, mais aussi d'intégrer l'exigence de sécurité by default dans les processus et les usages. Bref, de privilégier "l'expérience utilisateur"... Il ne s'agit donc en aucun cas d'opposer l'Humain aux technologies, mais au contraire de tirer le meilleur parti des deux : d'un côté, un utilisateur sensibilisé et responsabilisé ne chercherait plus systématiquement à contourner les règles de sécurité, et de l'autre des technologies plus "empathiques" s'adapteraient davantage aux besoins des utilisateurs et mettraient l'accent sur la sécurité des données au plus près de l'utilisateur.

Retrouvez le programme : ici.

Inscriptions gratuite et obligatoire : ici.

ACTUALITÉ

Vers un futur traité international contre l'utilisation des TIC à des fins criminelles ?

A l'initiative de la Russie, et malgré l'opposition des États-Unis, des Européens et de la société civile, l'Assemblée générale de l'Onu a adopté en Décembre 2019 une résolution controversée prévoyant la création en 2020 d'un comité intergouvernemental chargé de la rédaction d'un traité international contre "le recours aux technologies de communication et d'information à des fins criminelles".

Cette résolution adoptée par 79 pays (avec 60 États ayant voté et 33 qui sont abstenus) était co-parrainée par la Chine, le Belarus, le Cambodge, la Corée du Nord, la Birmanie, le Nicaragua et le Venezuela au nom d'un « vide juridique à combler »

Ses opposants y voient au contraire un moyen supplémentaire de restreindre l'utilisation d'internet et la liberté d'expression sur les réseaux sociaux liberté d'expression dans certains pays. Il existe en effet déjà un instrument international contraignant matière de cybercriminalité, la Convention sur la cybercriminalité, ou Convention de Budapest, entrée en vigueur en 2004.

Ils rappellent aussi que si contrairement au projet russe cette convention n'a qu'une portée régionale et non mondiale, elle sert toutefois aujourd'hui non seulement de référence pour les pays européens qui se dotent d'une législation sur la cybercriminalité, mais aussi de cadre pour la coopération internationale entre les États parties. Le projet russe pourrait, à terme, rendre obsolète la Convention de Budapest.

La **Direction générale des relations internationales et de la stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

À ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique (OMC)**, qui s'inscrit dans le contrat-cadre n°2018-02. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère des Armées
Direction générale des relations internationales et de la stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com