MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

Cultur'IA

Pour une intelligence de confiance au service de la sécurité

n°20

Mai - Juin 2024

CEND 2024
Cap IA

Edito

L'actualité de l'intelligence artificielle a été récemment marquée par les annonces du Président de la République dans le contexte du salon VIVATECH, annonces qui placent la France comme un pays leader au niveau européen sur le sujet. Du coté du ministère de l'intérieur et notamment de la Gendarmerie nationale, les initiatives à venir ne manquent pas au delà du développement de nouveaux projets, notamment dans le champ cyber. Parmi celles-ci, nous pouvons citer le hackaton, Hack GenAI qui se déroule au début du mois de juin sur la robustesse des larges modèles de langage, le partenariat avec 3 forces de gendarmerie pour développer une IA responsable au service du citoyen comme du gendarme ou encore l'organisation à venir au Campus Cyber de la conférence AI4GS dont vous trouverez le détail au sein de ce numéro. Cultur'IA a choisi de vous proposer un nouveau chapitre relatif à l'IA au sein des territoires, nous débutons cette aventure avec la région Provence Alpes-Cote d'Azur particulièrement dynamique. Et, nous ouvrons cet opus, avec une interview de Caroline Chopinaud, directrice du Hub France IA, qui rassemble un large écosystème en IA et promeut le partage de connaissances sur des thématiques en IA des plus diversifiées.

Général Patrick Perrot
Coordonnateur pour l'intelligence artificielle
Conseiller IA auprès du ComCyber-MI
Gendarmerie nationale

Caroline Chopinaud, *est titulaire d'un doctorat en Informatique (spécialité IA) dans l'équipe SMA du LIP6, en collaboration avec Thales et occupe depuis 2022 la fonction de* ***directrice du Hub France IA***

Quelle vision porte le Hub France sur les évolutions de l'IA dans les 5 ans à venir ?

Le Hub France IA a été créée en 2017. C'était une volonté de l'écosystème de se rassembler et de partager leur expérience et leur feuille de route IA, à une époque où les entreprises commençaient pour la plupart tout juste à industrialiser ces technologies. Il y avait à l'époque une vingtaine d'entreprises : des grands groupes, des startups et aussi quelques chercheurs et indépendants, tous assez experts du sujet.

Depuis, on a vu l'écosystème IA se diversifier, des institutions, des écoles spécialisés, des PME, ETIs qui se mettent à l'IA et même des cabinets d'avocats. C'est intéressant de voir que toutes les parties prenantes d'un projet d'IA se regroupent aujourd'hui au sein de l'association, avec toujours comme mission d'accélérer le déploiement de l'IA en France et aussi en Europe.

C'est assez difficile de dire de façon très précise où sera l'IA dans 5 ans. Qui aurait prédit il y a 5 ans que « tout le monde » aurait testé une IA à la maison, et aurait imaginé une telle accélération soudaine.

Ce qui semble évident aujourd'hui c'est qu'il est important de s'y mettre, de se former, de tester. L'IA n'est pas, n'est plus réservé uniquement à des profils techniques, on s'oriente de plus en plus vers de l'IA en termes d'usage.

Au fil des ans, on a vu arriver les algorithmes IA en open source sur du Sikitlearn puis Tensorflow à des modèles pré-entrainés sur étagère… et open source, alors dans 5 ans, on imagine bien de plus en plus de solutions IA clé en main et donc une appropriation beaucoup plus importante.

Le Hub France IA rassemble de nombreuses thématiques en IA pouvez vous nous en dire plus ?

L'association s'est donnée pour mission de fournir à l'ensemble du tissu économique français les clés pour accélérer sa croissance en IA. Pour ce faire, nous regroupons nos actions sous 5 grandes thématiques : IA de confiance, Adoption & Usages, Impacts, Ecosystème, Technologies.

En pratique, ces thématiques guident nos activités qui se déclinent en groupes de travail, en projets, en actions de veille et en événements. Tout notre enjeu, au-delà de couvrir ces grands axes, est d'identifier et produire les ressources utiles en IA, dans une démarche collaborative et de partage entre membres.

L'IA de confiance va s'intéresser aux normes et standards, aux aspects réglementaires, en particulier le fameux RIA (règlement européen sur l'IA), mais aussi à l'éthique ; sous adoption & usages, on entend sensibilisation, formation, usages sectoriels de l'IA dans une démarche responsable ; la thématique « impacts » quant-à-elle se préoccupe de l'impact sur l'environnement, la société, la transformation des métiers, c'est une thématique sur laquelle nous lançons des collaborations avec d'autres associations IA car elle est au cœur de beaucoup de questionnement actuellement ; la notion d'écosystème est importante pour l'association qui se veut fédératrice de l'écosystème IA français dans toute sa diversité, mais également avec une vision souveraine et européenne ; enfin, car l'IA est avant tout un ensemble de technologies, nous œuvrons pour une meilleur compréhension de ces technologies et de leurs mises en pratique.

Comment le Hub France IA travaille au dynamisme de l'écosystème en IA ?

Le Hub France IA c'est aujourd'hui environ 200 membres qui se regroupent pour faire avancer l'IA en France et en Europe, c'est en soit déjà un moyen de cultiver le dynamisme d'une partie de l'écosystème IA au travers d'activités et d'actions dédiées. Nos membres collaborent et partagent leurs expériences pour produire des livrables très concrets. Notre rôle est de les accompagner, de créer du lien et aussi de mettre en lumière les projets et les acteurs qui constituent cet écosystème.

C'est la raison pour laquelle par exemple nous menons depuis 4 ans, avec nos partenaires européens, un projet annuel de cartographie des startups en IA. En 2020 on référençait environ 120 startups, aujourd'hui nous référençons 328 fournisseurs innovants en IA, c'est un moyen de mettre en lumière ces acteurs et d'aider à s'y retrouver quand on cherche un partenaire, un fournisseur, une startup aussi dans laquelle investir… c'est utile pour tous.

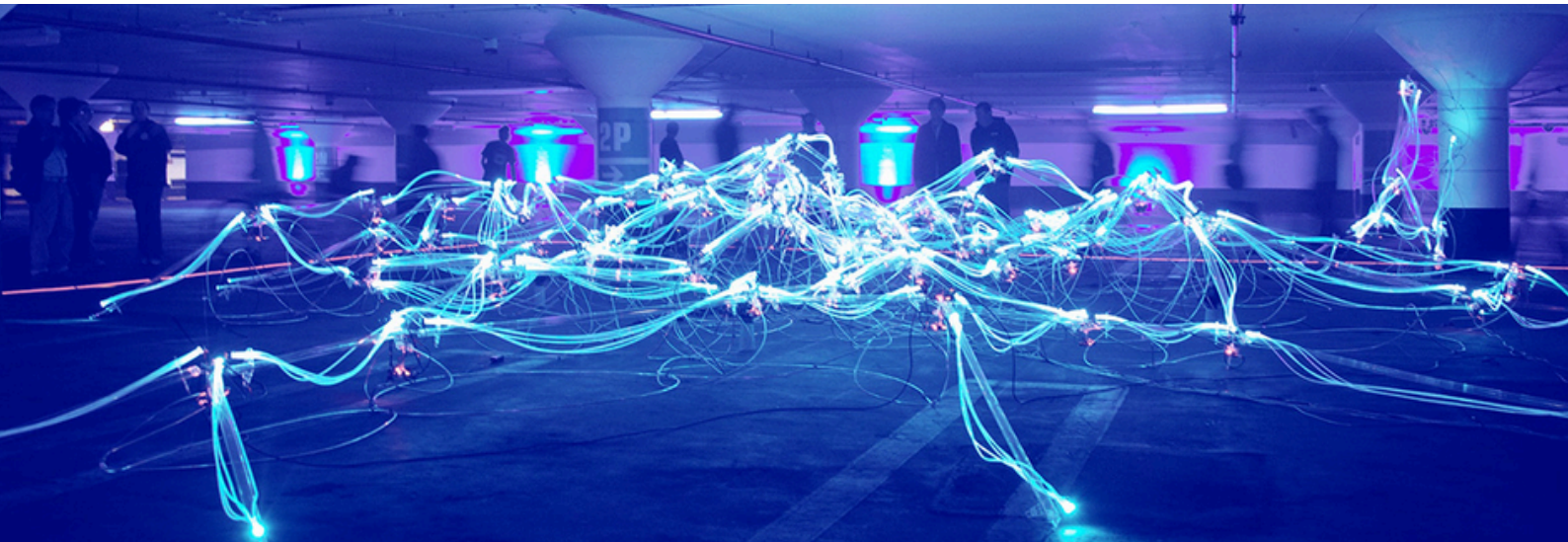
Aussi, toutes nos productions sont mises à disposition de tous, dans un esprit « open data ». C'est important pour nous et pour nos membres. Nous sommes tous convaincus que nos travaux doivent être largement diffusés. Nos membres progressent ensemble, ils partagent mais toujours avec comme objectif de produire des livrables opérationnels qui bénéficieront à tous, bien au-delà de notre communauté.

Mais c'est aussi, en travaillant avec nos partenaires en France et surtout en Europe (le Hub France IA est membre fondateur de l'association EAIF qui représentent 9 pays européens) que nous portons également la voix de nos membres sur des sujets stratégiques, comme l'AI ACT, le passage à l'échelle de l'IAG ou l'impact environnemental de l'IA…

L'IA générative bouscule les codes de l'IA en faisant craindre une IA omniprésente. Comment travailler à la confiance en cette discipline auprès de la population ?

Je réponds souvent à cette question comme ça : « ce n'est pas l'IA qui va vous remplacer, mais un humain qui sait se servir de l'IA mieux que vous ! ». Il y a une peur qui n'est pas totalement fausse face à l'IA. C'est normal, ce qu'on ne maitrise pas fait peur. Et puis, il y a beaucoup de « science-fiction » autour de l'IA, relayée grandement dans la presse et les médias. C'est un sujet facile pour faire le buzz et pour faire peur. Ce n'est pas nouveau ! Ce qui change avec l'IA générative c'est que tout le monde a pu tester (ChatGPT), tout le monde en a entendu parler sans tout comprendre et là, forcément ça amplifie aussi la peur : l'IA partout, l'humain qui perd son humanité, la perte du libre arbitre amplifié par les fakes news. Il y a effectivement de quoi se poser des questions. Pour travailler la confiance, l'europe a mis en place l'AI ACT, tout simplement déjà pour cadrer les usages de l'IA (au sens large). C'est un moyen de dire aux citoyens que ces technologies d'IA ne peuvent pas être utilisées n'importe comment et qu'il est nécessaire de s'assurer que les usages à haut risque, qui peuvent porter atteinte à l'intégrité humaine et aux droits fondamentaux, sont encadrés et réglementés.

Ensuite, à l'autre bout du spectre, il y a un vrai besoin de formation, a minima de sensibilisation. Pour ne plus avoir peur, il faut comprendre, il faut démystifier l'IA tout en maitrisant les risques. C'est alors qu'on peut vraiment se l'approprier. L'IA est un outil et sur certains sujets, c'est un outil vraiment très efficace. Il serait dommage de s'en passer !



HUB FRANCE IA

Le Hub France IA est une association à but non lucratif accélérant le développement et l'adoption d'une IA responsable, éthique et souveraine par l'ensemble du tissu économique.

Le Hub France IA, c'est 150+ membres et 50+ partenaires : start-ups, PME, ETI, grands groupes et institutions dont l'objectif est d'accompagner la stratégie nationale pour l'intelligence artificielle. Catalyseur de l'écosystème de l'intelligence artificielle en France, le Hub est présidé par Rim Tehraoui qui a succédé à Antoine Couret, celui-ci ayant quitté ses fonctions après six ans de mandat.

Les grandes thématiques de la feuille de route 2024 sont :

- IA de confiance ;
- adoption & usages ;
- impacts de l'IA ;
- écosystème et technologies.

Le Hub France IA est organisé en groupes de travail thématiques au sein desquels participe la Gendarmerie nationale pour certains d'entre-eux.

- AI Act
- Cybersécurité
- Banque et auditabilité
- Environnement
- Ethique
- Ressources humaines
- Chat-GPT
- Normalisation et IA
- Normalisation et IA
- Transport et logistique
- Voix et langage
- Formation

Dans le cas de ses travaux, le Hub a également proposé une cartographie des start-up européennes en fonction des thématiques spécialisées.

Après avoir publié une note de synthèse en mai 2023 sur les usages et les impacts de ChatGPT et de la GenAI, il a apporté dans ce rapport 40 propositions pour faire de la France et de l'Europe des leaders de la GenAI dans le respect des valeurs européennes.

4 objectifs principaux sont identifiés :

•Développer une approche holistique, respectueuse de l'environnement et des règles éthiques européennes, rassemblant fournisseurs, consommateurs publics et privés ;
• Anticiper les évolutions de l'IA en structurant le marché de l'accès aux données d'entraînement et l'architecture des supercalculateurs européens autour des prochaines ruptures ;
• Garantir un environnement qui permette l'émergence d'un marché réellement concurrentiel tout en préservant le marché des médias et de la culture ;.
• Apporter le soutien nécessaire à la montée en compétence mais également à la gestion des risques et la mise en œuvre des réglementations.

Rejoindre le Hub, c'est intégrer un écosystème diversifié et faire le choix du partage de connaissances et de bonnes pratiques pour une une montée en compétence.

L'IA, de nouvelles opportunités pour les cybercriminels

L'instabilité géopolitique actuelle et les échéances internationales à venir (élections européennes, Jeux Olympiques, élections américaines) constituent un terreau particulièrement fertile à l'essor d'une criminalité d'origine cyber. Les actions possibles ne manquent pas, tels tirer des bénéficies financiers, déclencher des actions de déstabilisation politique, d' expression d'opposition ou encore de manipulation de l'information,

Force est de constater que la hausse des attaques cyber et de l'essor des méthodes de « désinformation-as-a-service » (DaaS), transforment l'espace numérique en champ de bataille et aucun secteur, comme aucune personnalité ne sont épargnés. **Dans ce contexte, l'IA constitue une opportunité et un atout considérables aux mains des cyberdélinquants.**

Le panorama des cybermenaces s'accroît notablement et change de forme par l'intelligence artificielle. **Célérité accrue, ciblage augmenté et surface d'attaque croissante constituent quelques opportunités de l'IA pour les cybercriminels.** L'IA est aujourd'hui une discipline pluridisciplinaire qui peut être exploitée dans des champs des plus diversifiés démultipliant les possibilités d'attaques notamment sur des cibles peu protégées. Par ailleurs, le développement effréné des applications en IA à l'instar des larges modèles de langage néglige la sécurité et ouvre des failles considérables aux criminels.

- **Les attaques à partir des LLM**

Les LLM se sont largement imposés dans le domaine de l'IA pour dévenir incontournables aujourd'hui dans nombre d'applications citoyennes. Mais, ces LLM ont aussi un réel intérêt pour la criminalité. Ils sont exploités pour rédiger des e-mails de spear-fishing (hameçonnage ciblé) autant dans le domaine de la criminalité que de l'influence. **L'IA offre en effet une capacité de personnaliser des attaques en fonction de la cible recherchée et ces attaques peuvent être automatisées et confiées à des robots.** Ces LLM permettent aussi aux criminels de comprendre les caractéristiques des vulnérabilités des systèmes d'information, telle la faille CVE 2022 30190 de l'outil de diagnostic matériel de Microsoft. Les cyber criminels les exploitent également pour générer du code afin de compromettre des serveurs de données ou encore pour faire de l'ingénierie sociale et mieux connaître les entreprises. De telles pratiques démultiplient les capacités de réalisation des FOVI et s'adressent plus globalement aux enjeux d'intelligence économique. Ainsi, les LLM, permettent aux attaques d'exploiter l'ingéniérie sociale en automatisant les premiers échanges de mails personnalisés et de contourner les filtres anti-spam classiques.

- **Les attaques par exfiltration de modèles**

Les attaques par exfiltration de modèles consistent à récupérer l'architecture des systèmes d'IA, les hyperparamètres comme les paramètres pour dupliquer un système et ainsi mieux cibler des attaques. Ce "vol" d'IA peut bien entendu s'effectuer en mode "boite blanche" où, ayant accès au système, l'attaquant peut aisément réaliser une copie. Mais, c'est aussi possible en mode "boîte noire" en soumettant une succession de requêtes au système et, par analyse des réponses, en estimer le fonctionnement. Les taux de succès de cette forme de piratage peuvent aller jusqu'à 95%.

- **Les attaques adversariales**

Les attaques adversariales ont fait l'objet de nombreux travaux et témoignent de la capacité à totalement fausser l'interprétation d'un système d'intelligence artificielle sans pour autant que cela puisse être perçu par l'humain. Le principe consiste à injecter un bruit optimisé et imperceptible pour transformer la réponse de l' IA. Il est alors possible de prendre le contrôle d'un système et d'influer totalement sur son résultat.

A titre d'illustration, le visage d'un criminel sur un passeport lors d'un passage à l'aéroport pourrait passer pour "monsieur tout le monde" ou encore un panneau STOP pourrait être perçu, par un véhicule autonome, comme une limitation de vitesse à 110 km/h

- **Les attaques par empoisement des données**

L'empoisonnement des données durant la phase d'apprentissage des systèmes d'IA a pour objectif d'altérer la performance en influant sur le nombre de faux positifs comme de faux négatifs en injectant des données corrompues. A titre d'illustration, l'introduction d'images étiquetées comme "individus non pédophiles" dans des bases de données judiciaires pourraient ne plus permettre d' identifier les individus véritablement recherchés, le système s'entrainant sur de mauvais labels. Il est également possible dans la détection de spam, d'injecter des e-mails inoffensifs étiquetés et rendre le système moins efficace pour identifier le spam réel.

Ainsi, **l'IA offre aux criminels une capacité à multiplier les attaques, à les automatiser, à en réduire le coût, à accroitre la célérité et à minimiser les risques associées tout en maximisant les possibilités de profit.** Le nombre des attaques cyber ne cessent de croître, les attaques développées à partir d 'IA sont particulièrement difficiles à détecter et devraient augmenter encore le chiffre noir de cette délinquance. Les enjeux de réglementation seront essentiels pour doter les forces de sécurité intérieure des outils d'IA adaptés pour faire face à une exploitation délinquante de l' IA. Il en est de même au sein des entreprises où il apparaît nécessaire de s'interroger sur la pertinence des règles de sécurité actuelle face aux défis générés par ces nouvelles opportunités à base d'IA.

Le COMCYBER-MI et l'ISEP lance HACK GEN-AI, un hackathon dédié aux larges modèles de langage.

Dans le cadre des travaux de la chaire « IA et Sécurité », le Commandement du ministère de l'Intérieur dans le cyberespace (**COMCYBER-MI**) et l'Institut supérieur d'électronique de Paris (**ISEP**) organisent avec ses partenaires (**EUROPOL, MAGIC LEMP et LINAGORA**) du 31 mai au 2 juin 2024, sur le site de l'Institut supérieur d'électronique de Paris à Issy les Moulineaux, un hackathon dédié à l'attaque des larges modèles de langage. Il réunira des participants de toute origine (étudiants, professionnel, institutionnel, etc.) pour relever un défi qui s'annonce majeur pour les années à venir.

Face au développement exponentiel de ces derniers et de leur utilisation dans tous les secteurs d'activité de la société, il apparaît nécessaire de s'interroger sur la robustesse de ces outils mis à la disposition de tous et potentiellement à des fins malveillantes. C'est l'objet de ce hackathon qui associe l'approche opérationnelle à la pédagogie en :

- Évaluant la robustesse des LLM les plus utilisés à des attaques de type *prompt engineering*, comme d'empoisonnement des données
- Sensibilisant sur les fragilités de ces outils largement utilisés que ce soit en milieu professionnel ou à titre individuel.

Orientés et soutenus par des mentors de qualité issus de nos partenaires (EUROPOL, MAGIC LEMP, LINAGORA), vous travaillerez en équipe pour élaborer des stratégies innovantes d'attaques tout en respectant les directives éthiques. Vous aurez accès à des machines de calcul adaptées aux ambitions du challenge et des *datasets* seront proposés pour la tâche de fine tuning.

Passionnés d'IA, chercheurs et étudiants, rejoignez-nous (voir ci-dessous) et plongez dans le monde des LLMs afin de contribuer à faire progresser le domaine de l'intelligence artificielle !

Nous vous attendons nombreux pour deux journées passionnantes.

Magic LEMP
Bright minds for bright solutions

isep
École d'ingénieurs du numérique

COMCYBER-MI
« Nos forces, pour votre cyber-protection »

LINAGORA

EUROPOL
INNOVATION LAB

Information pratiques : Pour en savoir plus et s'inscrire à Hack Gen-AI
www.isep.fr/blog/event/hackathon-genai/

Date : du 31 mai au 2 juin 2024 **Lieu :** ISEP, 10 Rue de Vanves, 92130 Issy-les-Moulineaux.

AI4GS (Artificial Intelligence for Global Security)

Le 19 novembre 2024, l'association AI4GS (Artificial Intelligence for Global Security) propose une conférence au sein du Campus Cyber à Paris la Defense. qui rassemblera diverses thématiques dans le cadre de l'exploitation de l'intelligence artificielle au profit des enjeux de sécurité. Le programme accessible depuis https://ai4gs-24.ai4gs.org inclut les sujets suivants:

- IA en cybersécurité et l'UEBA ;
- Sécurité physique et analyse vidéo ;
- Analyse des réseaux sociaux et des sentiments ;
- Surveillance et cyberdéfense ;
- Détection d'anomalies dans les systèmes d'information;
- Détection automatique d'images à caractère pédopornographiques
- Analyse de la blockchain ;
- Détection de fraudes ;
- Réglementation et IA

Ces thématiques très larges, ont pour objectif d'embrasser le caractère transverse des systèmes d'intelligence artificielle et les nombreuses opportunités possibles en matière de protection des citoyens face à une criminalité technologique toujours plus sophistiquée.

L'appel à communication est d'ors et déjà ouvert et s'adresse aux universitaires, aux industriels comme aux institutionnels qui peuvent dès aujourd'hui proposer un résumé de leurs travaux sur le site de la conférence. Placée sous l'égide de l'IFIP, organisation internationale créée sous l'égide de l'UNESCO, **AI4GS organise cette conférence en partenariat avec le commandement du ministère de l'intérieur dans le cyber espace (Comcyber-MI), l'INRIA et l'AFIA**.

Les divers articles sélectionnés feront l'objet d'une publication au sein des éditions Springer dans la collection "IFIP Advances in Information and Communication Technology" (AICT). Après une sélection du comité de lecture, un article particulièrement pertinent se verra récompensé par les organisateurs.

CALENDRIER

- Date limite de soumission d'un résumé: 15 juin 2024
- Date limite de soumission de l'article: 15 juillet 2024
- Notification acceptation/rejet: 15 septembre 2024
- Date limite de version finale: 15 octobre 2024

Alors il n'est plus question d'attendre, valorisez vos travaux et n'hésitez pas à soumettre votre résumé dans les meilleurs délais.

COMCYBER-MI « Nos forces, pour votre cyber-protection »

Inria

AFIA Association française pour l'Intelligence Artificielle

AI4G4 : un groupe rassemblant 4 gendarmerie se rassemble pour construire une IA responsable et assurer une meilleure protection du citoyen.

Sous l'impulsion de 4 directeurs de gendarmerie (Italie, Espagne, Portugal et France) il a été envisagé en 2023, lors d'un rassemblement du G4 au Parlement européen de Strasbourg, de créer un groupe dédié à l'intelligence artificielle après ceux de l'environnement, du cyber et de la formation. Ce groupe existe désormais depuis les 22 et 23 mai 2024, il est né à Regua au Portugal où l**es membres experts de chaque pays se sont rassemblés pour définir une feuille de route et construire une IA responsable au profit d'applications opérationnelles**. Cette feuille de route répond à deux enjeux:

- **développer une IA responsable pour lutter contre le crime et assister les gendarmes** dans leurs activités quotidiennes tant sur le plan opérationnel que dans le champ des ressources humaines ou de la logistique.

- **prendre en compte les contraintes imposées par la réglementation européenne afin de sécuriser les usages de l'IA.** Conformément à l'ambition européenne, l'objectif n'est pas d'assimiler l'IA au simple usage d'un outil informatique mais de l'appréhender dans sa polyvalence en envisageant la formation du personnel comme le suivi en continu des systèmes.

Cette double ambition partagée par les 4 membres fondateurs permettra de sécuriser l'usage opérationnel des systèmes d'IA exploités par les forces de sécurité intérieure en veillant à la protection des libertés individuelles.

Le groupe, après la définition de sa feuille de route, envisage des actions très concrètes comme la rédaction d'une charte éthique, la mise en place de formations communes, la valorisation des actions par la publication d'une "newletters", la mise en oeuvre d'un site web, le partage de données non sensibles comme d'applications opérationnelles mais aussi la mise en oeuvre de challenges internationaux autour de thématiques propres aux enjeux de sécurité intérieure.

La création de ce groupe de travail renforce la nécessaire coopération sur des sujets d'aujourd'hui comme d'avenir face à une exploitation de l'IA toujours plus importante par la délinquance d'opportunité comme la criminalité organisée.

L'IA au coeur des territoires : la région Provence Alpes-Côte d'Azur

L'intelligence artificielle (IA) est un atout majeur pour le développement et l'avenir des territoires et apparaît comme un levier pour répondre aux enjeux économiques, sociaux et environnementaux actuels. Nous avons choisi pour ce numéro de présenter l'écosystème de la région Provence Alpes-Côte d'Azur (PACA) qui connaît déjà de nombreuses sources d'attractivité en matière d'IA. **En PACA, deux grands pôles se sont structurés autour d'Aix-Marseille et de Nice-Sophia**.

Le pôle Aix-Marseille s'oriente vers une action essentielle au développement de l'IA: les infrastructures. Il entend par exemple se positionner comme un hub international en Europe où convergent les fibres optiques des liaisons Internet. Cette situation en fait un lieu d'implantation de DataCenters avec un certain nombre de projets majeurs qui sortiront de terre dans les 5 années à venir.

Ce pôle regroupe un riche tissu économique et institutionnel, des acteurs majeurs ont décidé d'implanter leurs équipes au cœur de l'écosystème du fait des atouts développés ci-dessus.

- Enedis a implanté son laboratoire d'IA avec pour objectif d'améliorer sa performance opérationnelle. Ils alimentent en électricité 37 millions de clients et gère 1,6 millions de km de lignes. Ils sont implantés dans les locaux d'Aix Marseille Université au sein de la Cité de l'Innovation et des Savoirs Aix Marseille.

- L'entente Valabre qui regroupe de nombreux SDIS va se doter d'une structure IA pour détecter en temps réel les incendies sur le territoire national en moins de 30 mn au travers du projet prédictif Panoptes.

- La Chambre de Commerce et de l'Industrie a créé une entité, le rIalityLab pour faciliter l'intégration de l'IA au sein des entreprises des grands groupes comme des PME/ETI. Au regard des nombreuses demandes approximatives des entreprises, Aix-Marseille Université collabore avec le rIAlity Lab dans le cadre du projet européen MOVE2DIGITAL pour diagnostiquer le besoin réel en IA des entreprises. En fonction du niveau de confidentialité des données, le rIAlity lab procède au diagnostic pour proposer aux entreprises des solutions existantes sur le marché ou le développement de briques technologiques d'IA répondant au besoin.

Le développement de l'IA sur le pôle Nice-Sophia est conséquent, dynamique et très diversifié mais aussi plus récent que sur le site d'Aix-Marseille. **L'institut 3IA Côte d'Azur, porté par l'université Côte d'Azur, est l'un des 4 premiers instituts interdisciplinaires national en IA.** Il est particulièrement orienté autour de la santé et des territoires intelligents. Lancé en septembre 2019, l'institut a su fédérer entreprises, instituts de recherche et de formation et acteurs publics autour de l'intelligence artificielle.

En 2024, la communauté d'agglomération de Sophia-Antipolis créé un pôle de l'innovation qui participera au développement de la recherche appliquée comme de l'émergence de solutions technologiques: https://www.sophia-antipolis.fr/2022/09/30/pole-innovation/

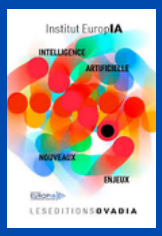
L'IA en PACA, c'est aussi l'Institut EuropIA auquel participe la Gendarmerie, la maison de l'IA, OTESIA et de nombreuses initiatives au service d'une IA inlcusive et pédagogique.

L'IA au coeur des territoires : la région Provence Alpes-Côte d'Azur

Des partenaires de la Gendarmerie nationale en région PACA

INSTITUT EUROPIA
COMPRENDRE POUR AGIR

Présidé par Marco Landi, l'Institut EuropIA, créateur du WAICF (World Artificial Intelligence Cannes festival), est une organisation à but non lucratif qui sensibilise et forme le public et les entrepreneurs à l'Intelligence Artificielle de manière éthique. L'objectif est de placer l'humain au cœur de l'IA, de valoriser l'écosystème local, et d'organiser des événements tels que des conférences et des Master Class. Plurisdisciplinaire dans son action, **l'Institut au sein duquel est partenaire la Gendarmerie nationale aborde de nombreuses thématiques dont les enjeux de sécurité.** Il est également à l'origine de nombreuses publications autour de thématiques des plus diversifiées comme l'éthique, les territoires connectés, la santé, l'espace, le tourisme, l'espace, les finances, l'art, l'internet des objets et bien entendu la sécurité.



WAICF
WORLD ARTIFICIAL INTELLIGENCE CANNES FESTIVAL

Depuis 3 ans se rassemblent au palais des festivals à Cannes, **de nombreux experts internationaux lors du WAICF auquel participe la Gendarmerie nationale qui fut la première institution publique présente.**

Le festival a ainsi permis de mettre en exergue les tendances mondiales : le développement des IA génératives, des modèles de fondation, de la durabilité, de l'open source de l'IA de confiance, de l'éthique, du Cloud ou encore de la sécurité des données. Après 3 éditions, le WAICF apparaît comme le premier rendez-vous mondial dédié exclusivement à l'IA, aux leaders de la tech qui y innovent et aux enjeux économiques, humains et sociétaux qui impacteront nos vies dans un avenir proche.

Cluster IA

Le ClusterIA est une association loi 1901 qui a pour vocation de réunir l'ensemble des acteurs de l'IA : grands groupes, centres de recherche et chercheurs, universités, institutions collectivités, PME & startups qui s'investissent dans le développement d'un écosystème IA. Il a été cofondé en mars 2019 sur l'initiative de Docaposte, filiale du groupe La Poste, et de Synchronext, aux côtés notamment de l'Université Côte d'Azur . Présidé par Alan Ferbach, CEO de Videtics, le cluster s'est fixé pour objectif de :

- Fédérer les acteurs azuréens de l'IA dans le but de les connecter, animer et accélérer
- Faire émerger des initiatives pour accélérer le développement de l'IA
- Être une interface de facilitation et de confiance pour les différents acteurs afin de développer des cas d'usage de l'IA opérationnels
- Promouvoir l'écosystème sur le plan national et international

L'IA au coeur des territoires : la région Provence Alpes-Côte d'Azur

Des partenaires de la Gendarmerie nationale en région PACA

MAISON DE L'INTELLIGENCE ARTIFICIELLE
DÉPARTEMENT DES ALPES-MARITIMES

La Maison de l'Intelligence Artificielle est une première en France et en Europe, **un lieu public de démonstration, de partage et de convergence des intérêts autour de l'IA.**
Elle permet à chacun de se plonger dans la découverte de cette technologie, de ses enjeux et des impacts sur nos modes de vie. C'est également un espace de dialogue mais aussi de coopération où peuvent naître et croître nombre d'innovations grâce aux données du territoire.

La Maison de l'Intelligence Artificielle (MIA) est un lieu où s'organise divers manifestations:

- visites pédagogiques (collèges) ;
- Elle est utilisable par les entreprises des Alpes Maritimes dans le cadre d'événementiel team building(*) ou séminaire si la thématique I.A est abordée ;
- Elle est utilisable :
  - par les associations des Alpes Maritimes dans le cadre d'événements de médiation, ou de formation à destination du public,
  - par des entreprises traitant des techniques de l'IA, de cas d'usages de l'IA, des impacts de l'IA ou de la découverte des métiers de l'IA ;
  - en tiers lieu numérique pour des groupes de réflexions ou afterwork(**) IA à destination des associations ou groupes universitaires ;
  - pour l'hébergement provisoire de start-ups(***) portées par des incubateurs des Alpes Maritimes ;

La MIA participe aux événements de médiation scientifique nationaux (fête de la science, ..)

POLE SCS

Créé en 2005, l'écosystème SCS est le cluster en Région Sud-Occitanie leader sur ces 5 axes stratégiques. L'Internet des Objets concentre les technologies clés portées par Pôle SCS et en particulier la sécurité des objets, des réseaux, des infrastructures cloud et technologies Big Data et IA indispensables au développement de ces marchés.

Les ambitions du pôle SCS s'articulent autour de:

- Génération des avancées technologiques significatives dans les domaines stratégiques en orientant l'activité de l' écosystème sur les enjeux d'innovation;
- Valorisation et déploiement des innovations technologiques dans les filières industrielles et les marchés qui peuvent en tirer un avantage compétitif, en convertissant les innovations technologiques en produits et services
- Etablissement de partenariats reconnus par les grands groupes internationaux, les pôles de compétitivité, les clusters et les institutions, afin d'engager l'écosystème industriel, et en particulier les TPEs/PMEs, sur des positions dominantes dans leurs marchés
- Renforcement des actions de soutien auprès des TPEs/PMEs en les accompagnant sur l'ensemble de leurs problématiques depuis l'innovation jusqu'à la commercialisation, dans le cadre d'un parcours de croissance, afin de permettre leur développement et l'emploi

La Gendarmerie est intervenue à diverses rencontres du pôle SCS autour de thématiques stratégiques et structurantes.

L'Institut 3 IA Cote d'Azur

Charles Bouveyron, Directeur du 3IA Cote d'Azur

L'Institut 3IA Côte d'Azur est l'un des 4 instituts interdisciplinaire d'Intelligence artificielle installés par le Président de la République en 2019, dans le cadre d'un appel à manifestation d'intérêt compétitif et après l'avis d'un Jury International, dans le cadre du plan « AI for Humanity ». Le 3IA Côte d'Azur est un consortium d'établissements de recherche et d'enseignement supérieur porté par Université Côte d'Azur, et composé d'INRIA, CNRS, INSERM, Eurecom et Skema Business School. En 4 ans, l'Institut 3IA Côte d'Azur s'est établi comme pilote de l'écosystème IA de son territoire, incluant entreprises et partenaires locaux, et a déjà acquis une forte visibilité au niveau européen et international.

Son ambition est à présent de devenir un leader mondial de la Recherche, de l'Innovation et de l'Enseignement en IA. Dans la première phase, l'Institut a mené des actions de recherche selon 4 axes : IA fondamental, IA pour la Médecine, IA pour la Biologie et IA bio-inspirée, et IA pour les territoires intelligents. Ces recherches ont donné lieu à plus de 900 publications scientifiques en 4 ans, dans les meilleurs conférences et journaux scientifiques internationaux, et ont permis de faire émerger des actions interdisciplinaires fortes, dont une grande partie ont été ou seront transférées à l'Industrie. En outre, l'Institut a été lauréat en 2019 de l'AMI « Compétences et Métiers d'Avenir » de France 2030 avec son projet EFELIA Côte d'Azur pour renforcer son action de formation en IA. L'Institut peut ainsi élargir et massifier son offre de formation en IA avec des moyens supplémentaires.

L'objectif de l'Institut 3IA Côte d'Azur est aujourd'hui de maintenir et d'accélérer la dynamique mise en place localement en IA, et de continuer à promouvoir les travaux de nos chercheurs et l'excellence de nos formations en IA au niveau international.

Fort de ses acquis, l'Institut redimensionnera et élargira son champ d'action dans les domaines de la Recherche, de l'Innovation, de l'Enseignement et de la Diffusion. Les 4 axes du programme de recherche de l'Institut ont été revisités pour d'une part répondre aux futurs défis de l'IA dans ces domaines, et d'autre part pour élargir les actions de l'Institut sur de nouveaux domaines applicatifs, tels que l'observation de l'Espace et la préservation de l'Environnement, la cyber-sécurité et la Physique. Cette extension thématique est motivée par les besoins futurs en matière de recherche et d'éducation des entreprises et des membres du consortium. Ce programme de recherche est aussi en ligne avec les priorités nationales sur l'IA embarquée et l'IA frugale, et sera coordonné avec les autres instituts du réseau.

La formation de l'Institut continuera de se concentrer sur des programmes d'excellence étroitement liés aux axes de recherche. Les objectifs de l'Institut en matière de formation sont de multiplier par 4 le nombre d'étudiants diplômés en 2030 de nos programmes d'excellence en IA.

L'IA au coeur des territoires : la région Provence Alpes-Côte d'Azur

Cet objectif sera atteint grâce à un consortium élargi à deux nouvelles grandes écoles françaises (Centrale Méditerranée et l'École de l'Air et de l'Espace), à des activités scientifiques consolidées sur les axes de recherche de l'Institut, à une stratégie visant à accroître le vivier de talents basée sur la visibilité internationale et la formation précoce des étudiants locaux, soutenue par un programme de diversité innovant, et à des liens plus forts et plus étendus avec les entreprises. Cette stratégie garantira l'attractivité des programmes de formation, tant au niveau européen qu'international.

Le programme Innovation sera également étendu afin d'accroître l'impact des programmes actuels qui fournissent un soutien à la création de startups et à l'ingénierie, et d'introduire de nouveaux produits pour soutenir les entreprises qui n'ont pas encore entamé leur transformation numérique vers l'IA. Une nouvelle action KickStart'AI ciblera les PME qui n'ont pas encore accès à la R&D dans le domaine de l'IA.

L'Institut mettra également en place des "chaires industrielles" en collaboration avec des entreprises intéressées à mener un projet de recherche à long terme avec des chercheurs de notre Institut.

En ce qui concerne les recherches en IA pour des questions de Sécurité et de Défense, l'Institut a déjà à son actif des résultats marquants, certains déjà exploités par les services de l'État, et va continuer les développements dans cette direction dans les années à venir.

Parmi les projets de recherche réalisés, on peut en particulier citer les algorithmes développés par Serena Villata pour la détection de la haine en ligne, la lutte contre le cyber-harcèlement et contre la désinformation, qui sont tous des sujets critiques à l'air de l'émergence d'une société de plus en plus numérique. Le projet Indago, porté par Charles Bouveyron, a pour objectif l'analyse non supervisée des réseaux de communication pour la détection des signaux faibles. Cet algorithme a notamment des applications pour le contre-terrorisme et la lutte contre la désinformation. Le projet SéquoIA, porté par Cédric Richard, exploite quant à lui les signaux spécifiques renvoyés par les fibres optiques déployées dans les villes pour la détection d'évènements (accidents routiers, mouvements de foule, glissements de terrains, crues) nécessitant l'intervention des services de l'État. Enfin, l'Institut 3IA Côte d'Azur porte par le biais de son groupe d'ingénieurs « data scientists » deux projets liés à la Sécurité et la Défense Nationale, en lien avec le SGDSN, pour le suivi et la détection en temps réel des sujets d'intérêt pour les services de l'État à partir des news publiés par les agences de presse (AFP, ...).

Charles Bouveyron, Directeur du 3IA Cote d'Azur

La page du réserviste

Romain Gémignani, ENEDIS, Réserviste opérationnelle au Comcyber-MI

La page du réserviste ouvre ses lignes à Romain Gémignani, LTN RS - expert IA, assisté de Nicolas Dunand expert national géomatique, d'ENEDIS qui parmi de nombreux travaux, nous présente celui de la détection et du géoréférencement des supports à partir d'images aériennes

Quel est l'objectif du projet ?

Enedis est présent sur 95% du territoire métropolitain pour acheminer l'électricité dans les foyers français. En tant que gestionnaire, l'entreprise pilote, raccorde, dépanne, entretient, développe et modernise le plus grand réseau de distribution d'électricité d'Europe. Les lignes à moyenne et basse tension, qu'on pourrait comparer à des « routes départementales » de l'électricité, représentent 1,4 million de kilomètres.

Ces dernières sont constituées de câbles conducteurs supportés par des poteaux. L'interface entre le conducteur et le support se nomme l'armement, ce dernier peut remplir différentes fonctions mécaniques et électriques.
La connaissance précise de la position et des armements des différents supports présente de nombreux avantages pour Enedis parmi lesquels nous pouvons citer : **l'accélération des dépannages, une meilleure politique de rénovation, une meilleure cartographie de nos ouvrages…** Toutefois, la tâche est ardue car le territoire à couvrir est immense (la quasi intégralité du territoire national) et le nombre d'objets à détecter colossal (de l'ordre du million).

La mise à disposition d'orthophotographies aériennes géoréférencées avec une définition de 5cm a permis à notre Laboratoire d'Intelligence Artificielle, situé à la Cité de L'Innovation et des Savoirs d'Aix-Marseille, de relever le défi par la mise au point de techniques innovantes uniques au monde.

De la photographie aux cartes, une histoire de tenseurs

Au sein d'Enedis, l'intelligence artificielle n'est pas une nouveauté. Nous avons développé plusieurs solutions d'IA au service de la performance industrielle, la transition écologique, les services aux clients ou encore la sécurité. L'intelligence artificielle nécessite des compétences avancées en mathématiques, ce projet ne fait pas exception. En effet, la cible étant de détecter, classer et rattacher chaque objet à des segments de réseau, il a fallu développer une suite d'opérations la plus optimisée possible pour garantir des temps de calcul et des besoins matériels raisonnables.

Ainsi, chaque image représentant un carré de 200mx200m est préparée avant d'être injectée à un modèle de détection d'objets combinant une double approche basée sur la photographie et la probabilité de présence de poteaux.

Ce modèle extrait l'ensemble des supports détectés dans l'image sous forme de position et de classe d'armement pour les fournir à l'algorithme de rattachement dont le but est de calculer le segment de ligne électrique le plus proche référencé dans notre système d'information géographique.

Chacune des étapes a fait l'objet d'un travail minutieux de nos équipes tant au sein des métiers que des experts en IA. Ainsi, pour entrainer le modèle, des experts du réseau aérien ont été sollicités pour labéliser plusieurs milliers d'images avant d'obtenir des résultats satisfaisants. Ce travail fastidieux est généralement essentiel dans tout projet d'IA et constitue un investissement souvent sans garantie de résultat de la part des services opérationnels.

L'algorithme de rattachement des objets aux segments de ligne a quant à lui nécessité plusieurs mois de travail conjoint de nos experts en IA et en géomatique. En effet, rattacher des millions de points à des millions de segments est une tâche complexe nécessitant de nombreuses astuces mathématiques et optimisations pour pouvoir être opérée de manière industrielle. Pour guider cette tâche, la contrainte matérielle a été déterminante : nous souhaitions pouvoir réaliser les calculs sur des GPU de 48Go de RAM maximum.

Cet algorithme consiste en suite d'opérations tensorielles[1] réalisées sur les GPU directement à la suite de l'inférence limitant ainsi les transferts de données entre la RAM de la machine et la RAM du GPU. Ce gain de temps, combiné à la parallélisation maximale des opérations sur GPU, a rendu le projet viable puisqu'au final il faut moins d'une heure de calcul pour couvrir l'ensemble de la zone géographique d'un département français et obtenir un fichier injectable dans notre Système d'Information Géographique.

Les contraintes rencontrées

L'algorithme de détection doit être exploitable sur l'ensemble du territoire français, avec des environnements d'implantation de poteaux très variés (zones urbaines / zones naturelles ; végétation septentrionale et méridionale).

Les typologies des poteaux sont également très diversifiées, selon la date de pose et les contraintes environnementales (poteaux en bois, doubles, haubanés, etc.) et présentent des orientations d'équipement multiples.

La simple approche académique de détection par image n'est pas suffisante pour ce type de situation et, avec un nombre d'annotations d'images raisonnable, il a donc été nécessaire d'utiliser à la fois un modèle peu sensible aux variations d'échelles, de rotations et de colorimétries, mais également d'adapter la courbe d'apprentissage aux techniques spécifiques de pose de réseaux (alignement, répétition, etc.).

De la preuve de concept à une démarche industrielle

L'ensemble des projets menés au sein du laboratoire d'IA d'Enedis Provence Alpes du Sud a une finalité industrielle. Cet objectif final dimensionne l'ensemble des étapes de développement des applications, ces derniers étant réalisés dans des environnements iso-production. Ainsi, dès lors que les résultats sont satisfaisants d'un point de vue métier, le transfert dans un environnement industriel est réalisé avec un effort minimum.

Dans cette situation particulière où le traitement ne sera à réaliser qu'une seule fois sur les données déjà en possession, le laboratoire d'IA sera chargé de traiter l'ensemble des données françaises et de fournir ainsi à la Digital Factory[2] un résultat exploitable pour une intégration dans les outils de l'entreprise. Cette nouvelle donnée sera une source pour de futurs travaux du laboratoire d'IA, tels que l'optimisation des installations de groupes électrogènes ou l'analyse des contraintes de la végétation sur les réseaux électriques.

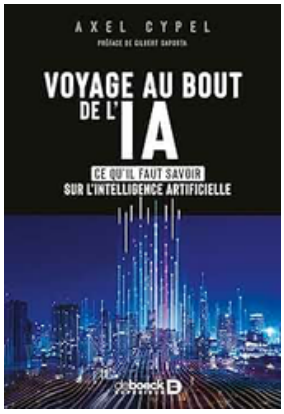
[1] Un tenseur est un tableau numérique à plusieurs dimensions souvent utilisé en informatique pour résoudre des problèmes complexes ou traiter des données volumineuses.

[2] Pour accélérer la création de valeur à partir de la collecte des données, depuis 2022, la Digital Factory structure une force de frappe cohérente en rassemblant toutes les compétences de l'entreprise.

Une mise en perspective intéressante d'une IA qui peut asservir si son utilisation est subie. En dépit de ses avancées, l'IA peut en effet diminuer l'homme par une mauvaise appréhension. L'auteur n'en n'oublie pas pour autant les potentialités positives de l'IA.

Loin de se limiter aux aspects techniques, FantasIA propose des textes drôles et pédagogiques, un voyage physique vers la Silicon Valley ou le Kenya mais c'est aussi un voyage de compréhension de nos fantasmes et de nos craintes les plus profondes sur l'intelligence artificielle.

La revue Actu IA consacre un dossier complet au enjeux de l'intelligence artificielle dans le domaine de la sécurité intérieure à l'échelle européenne, En effet les forces européennes se rassemblent autour de l'élaboration d'une stratégie commune.



Cet ouvrage présente une vision complète de ce qu'est l'intelligence artificielle et de ses enjeux notamment des IA génératives à l'origine d'un mélange d'inquiétude et d'espérance.

PODCAST & LITTERATURE

Plongez dans les conversations authentiques d'Anthony Romano avec les acteurs clés. Ce podcast est une immersion dans l'IA, racontée par ceux qui la façonnent.

Data Driven 101 : Sur Data Driven 101, Marc Sanselme s'intéresse aux applications pratiques de l'intelligence artificielle et de la data dans toute leur diversité avec un objectif : démystifier ces concepts. Ce podcast est une encyclopédie de bonnes pratiques, d'écueils à éviter et de cas concrets racontés par les invités.

Créé par la Cité de l'IA, ils compilent les témoignages d'experts et visent à aider les entreprises à appréhender le sujet de l'intelligence artificielle et à promouvoir toujours plus d'innovation. Ils permettent d'identifier, étape par étape, les conditions de réussite, freins et leviers pour intégrer l'IA dans son organisation

IA INFO

Annonce du Président de la République :

- doubler les investissements publics européens dans l'IA et le quantique;
- engager un dialogue social eclairé par la recherche;
- formation: engager des formations au sein des écoles en prenant en compte une vision éthique et promouvoir l'action à la consommation de l'IA;
- création d'un centre d'évaluation de la sécurité de l'IA;
- AI safety Summit aura lieu en février 2025 en France;
- De nouveaux clusters IA sélectionnés.

VIVA TECH 2024: outre la présentation des dernières initiatives en matière de technologie d'IA, VIVA TECH est l'occasion de nombreuses conférences accessibles depuis le site du salon. Arthur Mensh de Mistral AI est intervenu autour de l'IA de confiance et d'autres intervenants étaient présents comme Meredith Whittaker, spécialiste du domaine et présidente de la Signal Foundation, le journaliste de CNN Gianluca Mezzofiore ou encore Yann le Cun.

META: Lancement de LLAMA 3: Meta a lancé LLAMA 3 qui propose deux versions dont l'une avec 8 milliards (8b) ou 70 milliards de paramètres (70b) et qui se limite toujours à des requêtes et réponses textuelles. A ce jour 1800 invites couvrent 12 cas d'utilisation clefs : demande de conseils, brainstorming, classification, réponse à des questions fermées, codage, écriture créative, extraction, habiter un personnage, réponse à des questions ouvertes, raisonnement, réécriture et résumé.

SORA: Sora est le générateur de vidéos par IA développé par OpenAI, aussi créateur de ChatGPT et DALL-E. Cet outil permet, à l'aide d'une requête textuelle, aussi appelée prompt, de générer une séquence vidéo d'une minute maximum, répondant aux demandes de l'utilisateur en matière de style, de mouvements de caméra, d'effets, de personnages, etc

INRIA et LNE: Ces deux entités ont signé un partenariat pour la création d'un centre national de compétence et d'expertise public pour l'évaluation des systèmes d'IA

MISTRAL AI: Mistral AI a lancé un nouveau modèle, Mistral 8x22b, performant et rapide, avec un focus sur le multilingue, notamment le français.

ACTU IA: La seule revue francophone totalement dédiée à l'intelligence artificielle publie un dossier complet sur l'exploitation de l'IA au niveau des forces de sécurité intérieure européenne.

Culture IA

Au sommaire du prochain numéro

- Les réseaux de neurones récurrents
- Le hacking éthique
- La menace de l’IA en cyber
- L’IA au coeur des conflits
- La page du reserviste

Cap IA