Focus 5 – L’IA au service de la défense et de la sécurité

219

Focus 5 – L’IA au service de la défense et de la sécurité

Le domaine de la défense et de la sécurité s’intéresse depuis longtemps aux techniques d’intelligence artificielle sous leurs nombreuses formes : interfaces humain-machine, traitement de l’information, robotique, etc. Pourtant, ce n’est que récemment avec l’essor et la maturité croissante des technologies civiles que de nouvelles perspectives d’application s’ouvrent, aussi bien pour les besoins des phases opérationnelles dans le cadre de l’exercice des missions régaliennes que pour la transformation des activités internes au sein de l’État (par exemple pour les outils mis à dispositions des personnels des ministères). Dans les prochaines années, l’utilisation de l’intelligence artificielle sera une nécessité pour assurer les missions de sécurité, conserver l’ascendant face à nos adversaires potentiels, tenir notre rang par rapport aux alliés (aussi bien au sein de coalitions que dans une perspective d’export) et maintenir un niveau de qualité élevé concernant les services dispensés à l’ensemble des personnels des ministères.

La défense et la sécurité sont traitées ici de concert malgré les différences entre la nature des missions qui concernent notamment le ministère de l’Intérieur et le ministère des Armées. Une des différences réside notamment dans le lieu qui représente le théâtre du conflit : extérieur (opérations militaires), intérieur (sécurité intérieure) voire même virtuel (cyberdéfense). Du point de vue technologique, il semble cependant que les techniques d’IA développées pour l’une de ces applications ne la rendent pas moins transférable aux autres, et on peut noter de nombreux point de convergence notamment pour ce qui concerne le traitement de l’information. L’analyse d’images, de vidéos, d’enregistrements à titre d’exemple ne sont pas des techniques dont l’un des deux théâtres puisse revendiquer l’exclusivité. Les perspectives présentées ici se situent donc sur le point de convergence, mais nécessitent bien sûr une déclinaison opérationnelle plus précise qui prenne en compte leurs singularités.

On constate en l’occurrence que les caractéristiques et les besoins liés aux missions régaliennes sont souvent méconnus des acteurs du numérique (entrepreneurs ou chercheurs), qui en ignorent les enjeux, les problématiques et les opportunités. Si les ministères concernés jouent un rôle de premier ordre au regard de leurs données et de leurs usages opérationnels, les ressources humaines et financières dont ils disposent sont limitées. Ainsi, la collaboration entre le public et le privé est impérative et nécessite de voir émerger des écosystèmes de qualité. Le domaine est pourtant très mature et extrêmement riche en cas d’usage et données à haute valeur ajoutée pour des usages d’IA : imagerie (notamment satellitaire, drones, hyperspectrale), vidéos, signaux électromagnétiques (radars), systèmes de combat, renseignement, cybersécurité, robotique (aéronautique, marine, terrestre), données de maintenance, etc. Toutefois, pour des raisons légitimes de sécurité, de confidentialité et de faisabilité technique, il n’est pas toujours concevable de faire sortir complètement ces données du contrôle de l’État bien que le développement des technologies d’IA repose souvent sur l’alignement d’un triptyque connu : données, algorithmes et connaissances métiers. Accompagner l’écosystème dans la prise en main des problématiques du domaine, en particulier au travers de marchés publics relève d’un véritable enjeu de souveraineté

220

Focus 5 – L’IA au service de la défense et de la sécurité

Accompagner l’écosystème dans la prise en main des problématiques du domaine, en particulier au travers de marchés publics relève d’un véritable enjeu de souveraineté afin que, demain, nous ne soyons pas contraints de confier, comme cela a pu l’être par le passé, la réalisation de systèmes d’IA pour des besoins régaliens à des acteurs extra européens (exemple de Palantir). Le seul marché de la défense et de la sécurité n’étant pas toujours suffisamment large pour permettre aux entreprises du domaine de passer à l’échelle, il faudra garder à l’esprit que les technologies développées dans ce domaine ont vocation à être transférées à, ou depuis, des domaines civils connexes en tenant compte des intérêts essentiels de l’État. Les objectifs sont donc d’une part, de permettre à l’écosystème de recherche et d’innovation réunissant industriels de la Défense, communautés de recherche et entrepreneurs de travailler sur le domaine ; et d’autre part s’assurer que les innovations produites sont rapidement intégrées aux systèmes opérationnels.

Le développement de l’IA dans les domaines de la défense et de la sécurité intérieure ne peut néanmoins se faire de la même manière que dans d’autres secteurs. Dans un contexte marqué par ce qui est parfois dénoncé comme une forme d’inflation de lois sécuritaires, les risques liés notamment à la surveillance de masse et à la diminution des libertés publiques ne peuvent être négligés. Davantage que pour d’autres secteurs, les développements de ces technologies doivent s’insérer dans les débats politiques et, le cas échéant, les conséquences en termes de libertés publiques et d’éthique doivent être scrupuleusement étudiées.

La nécessité d’une IA régalienne et ses spécificités

L’IA crée avant tout une opportunité pour améliorer le quotidien de l’ensemble des métiers et des citoyens. Contrairement à certaines idées reçues, les premières applications identifiées relèvent de sujets du quotidien. Parmi les pistes, on peut évoquer : le filtrage des appels d’urgence arrivant aux 17-18112 pour désaturer, mieux prioriser et cibler ; la gestion de crise par la gestion des interventions et de l’information ; la réduction de l’accidentologie et du nombre de morts sur les routes. La réalisation de ces applications relève de l’intérêt général et en améliorant la qualité du service public et de son exercice.

Le développement et la mise en œuvre de techniques d’IA au sein des systèmes opérationnels sont de plus en plus cruciaux et concernent un spectre d’application large. Pour le traitement de l’information, le volume de données produites croît exponentiellement, la précision et la granularité des données produites par les capteurs augmentent et cette tendance ne va que s’accentuer avec le temps. Avec les ressources humaines disponibles, quand aujourd’hui on parvient à traiter une quantité de données qui avoisine au mieux les 20 %, à terme ce sera probablement moins de 2 %. Pour endiguer ce phénomène, il est donc nécessaire que les investissements réalisés dans le domaine des capteurs aillent de pair avec ceux dans l’IA permettant d’en exploiter la production. Cependant, bien loin de systèmes visant à automatiser les prises de décision, il s’agit avant tout de permettre à des opérateurs d’appréhender, de naviguer dans et d’exploiter la masse de données qu’ils ont à disposition. L’IA offre ici de nouvelles perspectives, car elle permet non seulement de mieux exploiter les données produites en

221

La nécessité d’une IA régalienne et ses spécificités

continu par les systèmes, mais également de mieux exploiter le patrimoine amassé efficacement. À titre d’exemple dans la recherche de contenu dans un ensemble de vidéos, quand il aurait précédemment fallu faire visualiser ces vidéos minute par minute par un ensemble d’opérateurs humains, il est aujourd’hui envisageable d’utiliser des techniques d’IA pour faire ce travail de façon automatique et beaucoup plus rapide.

La cyberdéfense et la cybersécurité évoluent dans ce même contexte de tsunami informationnel et de complexification constante des menaces. Si les moyens d’analyse automatiques permettent jusqu’à présent de détecter des attaques déjà connues, la mise en œuvre de techniques d’IA permet aujourd’hui d’imaginer des capacités de détecter, parer voire répondre à des attaques qui étaient jusqu’à présent inconnues. Alors que les modes opératoires des attaquants sont de plus en plus difficilement détectables par la seule capacité d’analyse des opérateurs humains du fait des temps longs et de la subtilité des signaux d’attaque produits, l’IA semble représenter une voie vers une meilleure protection de nos intérêts.

L’IA est également un moyen de protection pour nos forces et pour ceux qui assurent leurs missions au quotidien. Cette protection permet de faire face à des violences de différents types. Psychologique par exemple lorsqu’il s’agit d’effectuer de l’analyse de contenus qui peuvent être visuellement violents (vidéos de torture, images pédopornographiques dans le cadre d’enquêtes). Physique également lorsque des opérations mettent en jeu la sécurité des personnes : on peut citer à titre d’illustration la reconnaissance et la cartographie 3D de bâtiments en zone ennemie, ou encore le déminage (terrestre et maritime notamment) qui pourrait être effectué par des robots. Ces deux exemples montrent que dans certaines applications, il est possible d’utiliser des techniques d’IA pour préserver des êtres humains et limiter le niveau de risque auquel ils sont exposés. Dans le contexte du combat, l’IA permet d’outiller l’échelon de commandement pour faciliter l’accès à l’information et assister ainsi sa prise de décision, puis déssert localement les forces dans le contexte du combat collaboratif impliquant la connexion des différentes unités et moyens sur le champ de bataille. En amont, l’IA ouvre également des perspectives concernant la simulation opérationnelle qui permettrait à la fois l’entraînement des forces et la préparation des opérations. C’est enfin un facteur déterminant dans la performance et l’augmentation des systèmes de combat, notamment pour des fonctions support telles que la logistique et de la maintenance.

Quel que soit l’usage, les missions régaliennes nécessitent de prendre en compte certains aspects spécifiques pouvant être contraignants techniquement, notamment dans la conception des systèmes impliquant de l’IA :

– la sécurité et la protection des systèmes nécessitent d’être particulièrement renforcée et adaptée au contexte d’utilisation. En effet, les conséquences d’attaques en cas de vulnérabilité peuvent être importantes ; – la gestion des informations (classifiées à de multiples niveaux, éventuellement judiciaire), la protection du secret et du droit d’en connaître en particulier lorsqu’elles impliquent de grands volumes de données ;

222

Focus 5 – L’IA au service de la défense et de la sécurité

– l’interopérabilité avec d’autres systèmes, en particulier dans le cas de coalitions ou d’échanges internationaux ; – la répartition géographique des opérations et la multiplicité des modes de déploiements, de l’échelon central en métropole jusqu’aux théâtres d’opérations extérieures, y compris embarqués comme par exemple dans des bateaux ou des systèmes aéronautiques. – le besoin de fiabilité (entre humains, entre humains et machines...) et de contrôle accru dans un contexte où l’IA peut trouver sa place dans des applications critique (pilotage par exemple). – enfin, sur ces technologies qui évoluent à grande vitesse, il est impératif pour les techniciens et experts de se tenir au courant par la participation régulière à des forums, conférences, colloques internationaux, bien sûr dans le respect de la confidentialité qui s’impose aux actions les plus sensibles.

Il est évident que les expérimentations et les dérogations aux règles existantes, suivant la logique de bac à sable, doivent être effectuées dans le cadre strictement défini par le droit et sous le contrôle spécifique des commissions habilitées (notamment la commission nationale de contrôle des techniques de renseignement par exemple s’agissant du renseignement).

Dans un contexte où le besoin de souveraineté est critique, il faut souligner l’existence de réglementations telles qu’ITAR (International Traffic in Arms Regulations). Il s’agit d’une réglementation extra-territoriale américaine qui permet de contrôler les importations et exportations liées à la Défense. Elle s’exerce de façon rétroactive et concerne toute produit dont un élément de la chaîne de production a un lien avec les États-Unis. C’est pour cette raison que ces chaînes dans le milieu sont extrêmement contrôlées, dans la crainte que celles-ci puissent être soumises à une itarisation. La mise en place d’un environnement propice à l’expérimentation et au développement de l’IA

Afin de développer tout ou partie de ces usages, il faudra s’appuyer sur les logiques présentées pour le développement des secteurs prioritaires autour de la plateformisation, de la constitution de bacs à sable et d’une mise en place d’une politique de la donnée adaptée. Au vu du caractère exceptionnel de ses missions et de l’impératif de résilience, l’État, au travers notamment du ministère des Armées et du Ministère de l’Intérieur, doit conserver son autonomie sur les objectifs et les conditions de mise en œuvre de l’IA.

Pour des raisons historiques, les systèmes opérationnels actuels ne sont en majorité pas conçus pour mettre en œuvre cette démarche de recherche et d’innovation ouverte sur l’écosystème. Néanmoins, ce changement de paradigme est en cours au sein d’un domaine qui, à ce titre, est en avance par rapport à d’autres acteurs publics. Cependant, le déploiement d’une logique de plateforme qui consiste à expérimenter des capacités dans une phase de recherche et d’innovation, puis à les déployer sans rupture comme capacités opérationnelles demeure une entreprise délicate1.

La mise en place de logique de plateformes et de bac à sable nécessite notamment de développer un socle technologique adapté au domaine et qui tient compte des spécificités précitées. Son utilisation permettra de faire

1. Certains projets vont déjà en ce sens à l’image d’ARTEMIS pour le Ministère des Armées.

223

La mise en place d’un environnement propice à l’expérimentation et au développement de l’IA

support à la recherche, à l’innovation et au déploiement dans les systèmes opérationnels de briques d’IA, à condition que ce développement soit assorti des infrastructures nécessaires à sa mise en œuvre ainsi qu’à une démarche globale d’expérimentation qui implique l’alimentation en jeux de données, cas d’usage et campagnes d’évaluation. Ce mode d’expérimentation souple nécessite de constituer un bac à sable afin de fluidifier la possibilité de développer et de tester des produits opérationnels. L’objectif est notamment de permettre aux acteurs économiques d’aborder le domaine en bénéficiant de l’accompagnement nécessaire et du support de développement et d’expérimentation, au plus près des usagers. Ce bac à sable permettra de faciliter l’accès et l’utilisation de la plateforme mise en place pour développer de nouveaux usages s’appuyant sur des techniques d’IA, dans un cadre maîtrisé malgré la sensibilité du domaine. À cette fin, il faudra veiller à :

– permettre l’accès à des données opérationnelles dans un cadre maîtrisé par l’administration pour les acteurs économiques ; – produire des jeux de données d’intérêt exportables sur différents cas d’usage afin que la communauté puisse s’en saisir ; – créer un guichet unique d’instruction des dossiers pour la participation au bac à sable avec contrainte de délai de réponse.

L’importance de la dimension opérationnelle a été soulignée pour faciliter l’expérimentation et les développements au plus près des utilisateurs finaux. En effet, celle-ci est cruciale pour faciliter les démarches d’expérimentation, de conception itérative et de déploiement de produits. Ces démarches d’expérimentation sont indispensables pour tester des systèmes en conditions réelles, en particulier lorsqu’ils reposent sur des technologies qui intègrent de l’IA, et produire des systèmes pertinents pour les métiers du domaine de la défense et de la sécurité, développés à partir de cas d’usages réels. Pour y parvenir, il faudra permettre des expérimentations opérationnelles sur le terrain ou dans les centres d’essais2 pour donner vie à un living lab dans l’État3.

Cependant, les avancées de l’IA dans le domaine de la défense et de la sécurité dépendent notamment, comme pour les autres, de nos capacités à croiser des quantités massives de données afin de mettre en évidence des corrélations ou des motifs exploitables par des techniques d’IA. De ce fait, la quantité des données disponibles et la qualité de leur annotation sont des éléments clés pour faire avancer la recherche sur les applications de l’IA. Dès lors, il est essentiel de se doter des moyens de captation, de structuration et d’annotation des données produites. Pour cela, il faudra inscrire comme priorité à la fois financière et opérationnelle :

– l’organisation de la captation des données pertinentes ainsi que leur annotation/structuration à des fins d’IA puis en faire une priorité opérationnelle et financière ; – le renforcement du chantier mené sur la gouvernance de la donnée et la structuration de la connaissance à l’échelle du ministère ; – l’organisation d’une réflexion sur la classification de la donnée, les contraintes techniques et réglementaires dans un contexte d’IA pour créer un cadre réglementaire et organisationnel en adéquation avec les nouveaux usages liés à l’IA qui est parfois estimé en décalage dans la pratique.

2. Par exemple ceux de la Direction Générale de l’Armement pour le ministère des Armées.

3. Pour la Défense, le projet de « Défense lab » du Ministère des Armées devrait répondre à ces objectifs.

224

Focus 5 – L’IA au service de la défense et de la sécurité

Si la captation et le croisement des données sont évidemment nécessaires pour développer opérationnellement les applications d’intelligence artificielle, dans ces domaines particulièrement sensibles, ils pourraient avoir un certain nombre de conséquences négatives pour les libertés fondamentales. Une réflexion doit donc être menée, en amont de la collecte et du croisement, sur les risques éventuels qu’ils soulèvent. Ainsi dans le développement des systèmes de technologies d’IA, les bénéfices liés au développement de compétences opérationnelles doivent toujours être balancés avec les risques actuels ou potentiels qu’il font peser sur les libertés individuelles.

Une gouvernance et un cadre à consolider

Les ministères régaliens sont déjà sensibilisés aux enjeux de l’IA et du numérique en général et se sont déjà structurés ou restructurés en conséquence. En matière de gouvernance, l’enjeu est de parvenir à créer une synergie favorable à l’innovation (de la phase recherche au déploiement dans les systèmes opérationnels) à travers la mise en œuvre de dispositifs de collaboration entre les utilisateurs et les directions techniques concernées. Le Ministère des Armées par exemple, du fait du découpage institutionnel a déjà mis en œuvre un dispositif à cette fin au travers du Défense Lab qui réunit Direction Générale de l’Armement, Direction Générale du Numérique et des Systèmes d’information et de communication et État-major des Armées. Pour le Ministère de l’Intérieur, la direction des systèmes d’information et de communication porte le projet technique en lien direct avec les métiers.

La question des ressources humaines mérite une attention spécifique, bien que le secteur soit déjà acculturé en grande partie à la problématique. En particulier, l’IA va induire de nombreux changements pour les métiers, et demande ainsi un travail de terrain au contact des utilisateurs, à la fois pour permettre de faire émerger les applications les plus pertinentes du point du vue opérationnel mais également pour amorcer les cycles de transformations à venir en y impliquant d’emblée les utilisateurs finaux. Ce travail ne pourra se faire que dans un contexte de sensibilisation à tous les niveaux aux enjeux de l’IA, qui implique donc globalement une montée en compétence de l’ensemble des ministères, des Administrations et des États-majors. La montée en compétence passe en particulier par la dotation en équipes spécialistes en matière d’IA capables d’appréhender simultanément les enjeux des métiers opérationnels et les nouvelles technologies. Il faut également souligner l’importance de disposer de budgets dédiés à l’IA et au numérique afin d’être en mesure d’expérimenter et de lancer des projets pilote.

De même que l’IA apporte une rupture technologique avec l’existant, elle impose de reconsidérer un héritage historique réglementaire et organisationnel qui pourrait freiner son développement artificiellement. Au-delà des recommandations générales concernant par exemple la mise en place de budgets dédiés et pluriannuels transverses à l’ensemble des Administrations, deux points sont particulièrement saillants. Le premier concerne la classification et la déclassification des données et ainsi la possibilité de leur partage avec l’écosystème : la protection de l’information classifiée dans le numérique mérite une réflexion approfondie afin d’en simplifier l’appréhension à l’aune des nouvelles technologies. En particulier, des mécanismes de déclassification

225

Une gouvernance et un cadre à consolider

automatiques pourraient être étudiés afin de faciliter les développements de techniques d’IA nécessitant des données : date de péremption de la classification, déclassification massive, transformation systématiques et préidentifiées de la donnée en réduisant le niveau de sensibilité (par exemple lorsque la classification est issue des caractéristiques techniques des capteurs), etc. Le second porte sur la réglementation concernant la sécurité des systèmes d’information en vigueur. Si l’esprit n’est pas remis en cause, il faudra examiner certaines pratiques et déclinaisons qui pourraient être revues pour repenser des contraintes de sécurité adaptées au contexte IA et big data.