

## IA et robotique : une convergence qui s'accélère



**GBR Patrick PERROT**  
*Inspecteur général*  
*Gendarmerie nationale*  
*Senior advisor du CyberCercle*

L'intelligence artificielle (IA) et la robotique sont à l'origine de nombreux fantasmes depuis de longues années, qu'il s'agisse des mythes de l'être artificiel pour l'une ou des prouesses technologiques des automates pour l'autre. Ces deux disciplines ont longtemps évolué en parallèle sans réellement converger : la robotique portée par une volonté d'agir sur le monde physique, l'IA se déployant de plus en plus dans l'espace cognitif. Les avancées scientifiques et technologiques récentes, renforcées par les applications opérationnelles au sein des nouvelles formes de conflictualité, marquent aujourd'hui le temps de leur convergence, une convergence qui ne devrait cesser de croître.

Depuis le début des années 2000, l'essor des architectures d'apprentissage profond, associé à l'explosion des capacités de calcul et à la disponibilité massive des données, a rapproché les trajectoires d'évolution de l'IA et de la robotique. Plus récemment, l'effervescence autour des grands modèles a ajouté une dimension supplémentaire au lien entre IA et robotique : l'autonomie, qui ne doit pas être confondue avec l'automatisation limitée à

l'exécution de tâches selon des règles établies. Longtemps considérée comme une limite à ne pas transgresser, l'autonomie ne peut plus être considérée comme une frontière infranchissable. Un robot a longtemps été cantonné à l'exécution de tâches déterministes et répétitives ; il est désormais un agent capable de s'inscrire dans un environnement, d'adapter son action en minimisant ses erreurs (autonomie opérationnelle), et d'agir sans solliciter le consentement humain (autonomie décisionnelle). Nous pouvons alors nous interroger sur la forme de gouvernance des robots autonomes à mettre en œuvre afin de préserver la responsabilité humaine sans renoncer aux gains opérationnels de l'autonomie ?

En effet, l'évolution de la robotique n'est pas anodine : elle redéfinit les modalités de la décision comme de l'action, déplace les lignes de la responsabilité, et interroge la gouvernance autant que la souveraineté scientifique et technologique. Le sujet n'est plus de savoir si l'humain restera « dans la boucle » de chaque action élémentaire, il n'y est déjà plus dans bien des situations. Le sujet est de définir à quelles conditions il demeure l'orchestrateur légitime de la chaîne de décision : celui qui fixe les objectifs, borne la capacité autonome, arbitre les exceptions et assume la responsabilité finale.

### **De l'intérêt de l'IA en robotique : du robot exécutant à l'agent décisionnaire**

Ces dernières années, la robotique a considérablement évolué par l'intégration progressive de l'IA qui a apporté des changements significatifs dans l'architecture d'un robot et déplacé le centre de gravité vers plus d'autonomie. De manière simplifiée, un robot peut se décomposer en trois grands modules :

- une instance de captation : la capacité à recueillir

des informations sur l'environnement et à estimer un état en vue d'une action de commande ;

- une instance d'action : la capacité matérielle à agir ou à interagir avec l'environnement ;
- une instance de contrôle : la capacité de choisir et de mettre en œuvre une action ou un comportement en fonction de l'objectif assigné, de l'adaptation de l'état du robot à son environnement.

L'IA apporte une plus-value sur chacun de ces trois modules, mais c'est au niveau du contrôle que les progrès sont les plus considérables, par le développement de capacités d'évaluation, de choix et de décision face à un environnement et un objectif donnés. Les robots deviennent ainsi des systèmes capables de répondre à des tâches de plus en plus complexes, et cela dans des domaines des plus variés et avec une capacité autonome de décision. Ils ont toujours permis d'accroître la célérité de l'action et d'éviter d'exposer l'humain à des situations dangereuses ; mais désormais, dans certaines situations, le robot peut planifier, concevoir, créer et sous condition décider.

C'est précisément ce déplacement du contrôle de la règle programmée vers la décision pré-entraînée qui explique le chemin vers l'autonomie. Cette robotique de plus en plus autonome trouve d'ailleurs dans les derniers conflits un théâtre d'expérimentation très concret qui en facilite à la fois l'adoption et l'évolution.

### **Les conflictualités, catalyseur de l'essor de l'IA en robotique**

L'essor de l'IA au sein de la robotique s'est particulièrement révélé à travers l'évolution du contexte géopolitique, marqué par les récents conflits en Ukraine ou au Moyen-Orient. L'IA y joue un rôle d'accélérateur manifeste en matière de technologie, et notamment de robotisation. L'usage des drones autonomes en est certainement l'illustration la plus concrète, avec une accélération

des applications opérationnelles. L'autonomie létale n'apparaît plus comme une ligne infranchissable : l'action du drone reste souvent programmée par l'humain, mais elle est de plus en plus déclenchée à partir d'une reconnaissance automatique d'images, préalable au tir engagé par le drone lui-même que ce soit en zone terrestre comme aérienne en Ukraine ou maritime dans le détroit d'Ormuz. Il est difficile de disposer de chiffres stabilisés et fiables mais le ministère de la Défense ukrainien a récemment rapporté 22 000 missions accomplies par des robots terrestres autonomes sur seulement trois mois. Fort des enseignements tirés, le Pentagone a lancé aux Etats-Unis le programme « Replicator » dont l'objectif est le déploiement de flottes de drones autonomes à faible coût, en mesure d'opérer en essaim à des fins de saturation de l'ennemi. Les conflits récents n'expliquent certes pas à eux seuls la convergence IA robotique, mais ils en constituent un accélérateur et un révélateur particulièrement visibles.

L'impact des rivalités géopolitiques sur l'évolution technologique ne peut en effet être considéré comme totalement nouveau, il était même peut-être plus déterminant lors de l'émergence du quantique, du nucléaire ou de l'informatique. Ce qui change néanmoins aujourd'hui, c'est le rythme : les cycles d'innovation s'accélèrent, tandis que la capacité collective à les absorber diminue. Dans le même temps, la diffusion de ces technologies au sein de la société civile croît inexorablement. Alors que la géopolitique relevait largement d'enjeux militaires, elle est désormais portée, de plus en plus, par le secteur civil, modifiant par là même, les règles de droit jusqu'alors circonscrites aux conflits armés. L'IA irrigue aujourd'hui les applications robotiques civiles dans des domaines aussi divers que la sécurité, l'économie, la logistique, l'agriculture ou la chirurgie.

L'essor de l'IA au sein de la robotique n'est donc pas une trajectoire technologique neutre : elle bouleverse les équilibres, interroge le contrôle des

systèmes, des puces comme des données, dépasse largement le cadre des Etats, et génère des externalités comme des dépendances technologiques difficilement réversibles. Or, c'est précisément cette montée de l'IA en robotique qui ouvre, en miroir, un nouveau front de vulnérabilité : celui de la cybersécurité.

### **L'émergence de nouvelles vulnérabilités cybernétiques**

Par un réflexe anthropomorphique, la robotique est trop souvent assimilée à une forme humaine, voire animale. En réalité, elle constitue, lorsqu'elle est augmentée par l'IA, un champ d'application considérable et, par conséquent, une source de vulnérabilités nouvelles dans l'espace cyber. A l'instar de leurs homologues « droniens », des essaims d'agents IA peuvent déclencher des actions de neutralisation, par effet de saturation, des systèmes d'information à partir d'une analyse autonome du comportement des objectifs ciblés. Cette logique peut également être appliquée à des fins défensives où un agent autonome peut être utilisé pour protéger lui-même son propre système d'information. A titre d'illustration, un agent embarqué sur un robot de maintenance industrielle pourrait détecter en temps réel une tentative d'intrusion sur son propre firmware et déclencher automatiquement un isolement réseau ou une réinitialisation sécurisée, sans attendre l'action d'un opérateur.

Trop souvent perçue comme un simple amplificateur d'attaques déjà existantes, l'IA est en réalité aussi génératrice de formes d'attaques nouvelles, plus difficiles à détecter, plus rapides à exécuter, et qui dépassent largement le cadre des menaces informatiques conventionnelles. L'IA n'augmente pas seulement la vitesse ou l'échelle de certaines attaques, elle déplace la vulnérabilité vers les systèmes de perception, d'interprétation et de décision embarqués dans les robots. L'intégration

de l'IA introduit ainsi de nouveaux vecteurs d'attaque, qui amplifient significativement la surface d'exposition aux menaces cybernétiques et fragilisent de nombreuses applications. L'exemple de Mythos d'Anthropic a révélé la capacité de l'IA à mettre à jour les failles systémiques. Associer cette capacité à des essaims de robots dans l'espace cyber remet totalement en cause les capacités de protection préventive. En dotant les robots de capacités perceptives, adaptatives et décisionnelles, l'IA accroît considérablement les vulnérabilités au niveau même de la tâche de contrôle. Un robot chirurgical assisté par IA pourrait voir ses capteurs corrompus par une injection de données falsifiées, transformant une vulnérabilité numérique en atteinte physique. Dès lors que les domaines d'application sont sensibles ou régaliens, l'exposition aux attaques cyber devient un enjeu stratégique de premier plan. La sécurité reste encore trop souvent négligée au profit de la performance et de l'agilité. Il s'agit d'un déséquilibre d'autant plus risqué que c'est cette même autonomie décisionnelle, censée apporter de la valeur, qui devient le point d'entrée privilégié de l'attaquant.

Cette double lecture ayant trait à l'autonomie comme source de performance rejoint une question plus large, qui dépasse le strict champ technique : celle de la place que conserve, ou que perd, la décision humaine dans des fonctions qui engagent.

### **Vers un risque de déshumanisation de l'action comme de la décision**

S'il est une question qui demeure fondamentale dès lors que croît la convergence entre l'IA et la robotique, c'est bien celle de la déshumanisation de l'action comme de la décision. La réponse à cette question pourrait voir se substituer à l'intentionnalité humaine un processus algorithmique autonome, dans des domaines qui définissent, par essence, le contrat entre l'Etat et le citoyen.

La mise en œuvre concrète de cette convergence relève, en matière régalienne, d'un point d'équilibre autour de la juste mesure de l'autonomie et de la capacité à la contrôler. La délégation humaine au robot peut être partielle, à partir d'un robot fortement pré-configuré par l'IA, ou totale, le système agit seul, en temps réel, sans possibilité d'interposition humaine.

La convergence entre l'IA et la robotique emporte donc bien un risque de déshumanisation mais elle peut tout autant être employée pour redonner du temps à la décision comme à l'action humaine : une forme de ré-humanisation de certaines tâches, en libérant la charge cognitive. Dans le champ de la sécurité, un enquêteur qui n'a plus à traiter manuellement des téraoctets de données peut concentrer sa réflexion sur ce qui requiert un réel apport humain : la conduite d'une audition, la compréhension d'un contexte, l'évaluation effective d'une dangerosité, une meilleure interprétation des éléments de preuve.

L'usage de robots rendus autonomes par l'IA doit ainsi répondre à une exigence de subsidiarité, et non de substitution technologique : l'outil n'est utilisé que là où il apporte une valeur ajoutée mesurable, contrôlable et auditable. Cette exigence de subsidiarité n'est cependant qu'un principe ; elle ne garantit rien par elle-même. Reste à savoir comment elle se traduit concrètement dans l'organisation, et quel rôle l'humain y occupe réellement au regard des évolutions à venir.

### **Du contrôle à l'orchestration : repenser la gouvernance à l'ère des robots autonomes**

Les organisations doivent s'orienter vers un modèle de gouvernance qui combine la supervision, la compréhension et la résilience, afin de distinguer l'autonomie acceptable de celle qui est nuisible. Cela suppose de définir précisément quels agents IA sont autorisés à interagir avec quels systèmes, de

mettre en place des contrôles au niveau des protocoles de communication, des architectures réseau et de la couche d'identité, de concevoir des défenses capables de s'adapter à l'évolution des robots eux-mêmes et de s'engager vers l'auditabilité de l'ensemble.

La vraie question n'est donc pas tant celle de la déshumanisation que celle du contrôle : qui décide, qui surveille, qui peut interrompre le processus ? Cette question engage autant les juristes, les métiers et les citoyens que les ingénieurs. C'est à cette condition seulement que la convergence IA robotique pourra être un outil au service de l'humanité contribuant à une meilleure subsidiarité.

Pour les organisations, cette exigence de gouvernance se traduit par un changement de posture plus profond qu'il n'y paraît. Tant que le robot exécutait, l'humain supervisait directement chaque action : il restait, en quelque sorte, l'opérateur. Mais à mesure que les robots deviennent des agents capables de percevoir, de décider et d'agir de façon autonome, parfois en essaims, parfois en coordination avec d'autres agents logiciels, la supervision directe, action par action, devient matériellement impossible. L'humain ne peut plus être dans la boucle de chaque décision élémentaire, il doit se positionner hors de la boucle afin d'être au niveau de celui qui définit les objectifs, fixe les limites, arbitre les priorités et intervient sur les cas qui l'exigent.

C'est très exactement le rôle de l'orchestrateur : non plus celui qui exécute ou qui supervise chaque tâche, mais celui qui décompose une mission en sous-tâches, qui détermine quel agent, humain ou artificiel est le mieux placé, qui fixe les règles d'engagement et les seuils d'alerte, et qui recompose, in fine, les résultats en une décision assumée. Demain, au sein du champ régalien comme dans l'entreprise, l'humain n'agira plus en exécutant unique face à une machine isolée : il agira comme

l'orchestrateur d'une flotte d'agents, certains robotiques, certains purement logiciels, dont il devra garantir la cohérence d'ensemble, la traçabilité et, in fine, assumer la responsabilité de l'action comme de la décision.

Ce glissement n'efface ni le risque ni l'exigence de vigilance évoqués plus haut : un orchestrateur mal conçu, mal surveillé ou trop largement délégué reproduirait, à plus grande échelle, les mêmes risques de déshumanisation et de vulnérabilité cyber. Mais bien gouverné avec des règles d'engagement claires, des points de contrôle identifiés et une capacité d'audit réelle, ce rôle d'orchestrateur est précisément ce qui permet de concilier l'échelle et la rapidité qu'apporte l'IA en robotique avec le maintien d'une intentionnalité humaine au sommet de la chaîne de décision.

### **Conclusion**

La convergence entre l'IA et la robotique n'est plus une hypothèse de travail : elle est à l'œuvre, accélérée par la conflictualité contemporaine, et elle redéfinit en profondeur ce qu'un robot fait, ce qu'un système d'information protège, et comment peut évoluer la décision humaine. Le fil qui relie ces trois aspects est unique : le déplacement du contrôle, de la règle vers l'autonomie décisionnelle, qui crée à la fois la valeur et la vulnérabilité.

Pour les organisations, l'enjeu n'est donc pas de freiner cette convergence, ni de l'accueillir sans condition, mais de redéfinir la place de l'humain à mesure qu'elle progresse. Cette place ne sera plus celle de l'opérateur qui agit, ni même seulement celle du superviseur qui valide : elle sera celle de l'orchestrateur, qui conçoit l'architecture de la décision, répartit la capacité autonome entre agents humains et artificiels, et reste seul comptable du résultat. C'est à cette condition que la convergence IA robotique demeurera un outil au service de la décision humaine, et non de sa dépossession.

L'enjeu aujourd'hui est de savoir si nous nous plaçons à l'initiative, en situation de maîtrise, ou si nous choisissons d'être en position de vassalisation. Cette évolution est une véritable transformation stratégique qui nécessite de repenser le rôle et le niveau requis de l'humain en qualité d'orchestrateur, la redéfinition des tâches et emplois, la mise en place de formations adaptées sans omettre la responsabilité et le cadre juridique. C'est à n'en pas douter l'enjeu des quelques années à venir.