



cortAix

Artificial Intelligence by THALES

Intelligence Artificielle

pour les centres
de commandements et contrôle

THALES
Building a future we can all trust

Intelligence Artificielle

pour les centres de commandements et contrôle

Avec les contribution de: Patricia Besson, Sébastien Chenebeau, Philippe Gasc, Katarzyna Kapusta, Jérôme Kodjabachian, Anthony Larue, Christophe Lebreuche, Aldo Maalouf, Hélion du Mas, Juliette Mattioli, Christophe Meyer, Jaime de Oliveira, Arnaud Samama, Claire Trefoux, Matthieu Walle, Cyrille Guetin

Résumé

L'IA transforme les systèmes C2 en outils plus rapides, intelligents et adaptatifs, essentiels face à la complexité croissante des conflits modernes. Elle améliore la prise de décision, automatise les tâches, permet d'anticiper les menaces et d'optimiser la manœuvre. Les nouvelles générations de C2 intègrent des modules IA et des chaînes MLOps dans des architectures adaptées. Thales propose des solutions robustes face aux nombreux défis posés par l'intégration de l'IA dans les C2. L'IA reste un assistant : elle soutient le commandement sans le remplacer, en renforçant l'efficacité opérationnelle tout en respectant la hiérarchie militaire.

1. Qu'est-ce qu'un C2 ?

L'OTAN, dans ses documents de référence tels que l'Allied Joint Publication AJP-3, définit ainsi le Command and Control (C2): "C2 is the exercise of authority and direction by a properly designated individual over assigned and attached forces in the accomplishment of the mission."

Le C2 englobe plusieurs fonctions et capacités essentielles :

- Prise de décision, incluant la planification, l'organisation, la direction et le contrôle d'opérations militaires.
- Transfert d'informations : échanges d'ordres, de rapports et de renseignements nécessaires à l'action.
- Systèmes C2: infrastructures, procédés, réseaux et moyens techniques permettant au commandement d'assurer l'efficacité et la coordination des forces.

La doctrine française définit ainsi le C2 en page 9 du document DIA-3.0_CEO_L1_HTN (2019) :

- Le commandement est une responsabilité confiée à un militaire associé à une autorité nécessaire pour analyser, comprendre et apprécier une situation, concevoir, organiser planifier, donner des ordres, diriger l'exécution, évaluer les résultats.
- Le contrôle est inclus dans le commandement, elle est l'autorité qui dirige l'exécution et évalue les résultats.

Un SI C2 vient à l'appui d'un processus métier tel que la MEDOT (Méthode d'élaboration des ordres tactiques) dans l'Armée de Terre ou COPD à l'OTAN, repose sur la détermination d'un effet à obtenir et permet de structurer les actions. Le SI C2 est connecté à des senseurs (caméras, radars, station météo...) et à des systèmes d'armes. Le SI C2 est hébergé sur des infrastructures de nature diverse, depuis le datacenter au calculateur embarqué (véhicule blindé, aéronef, navire, UxV). Le SI C2 dispose d'une connectivité adaptée à ses besoins d'échanges (portée, débit, latence, résistance aux menaces cinétique, brouillage).

Les fonctions d'un SI C2 sont nombreuses :

- Renseignement multi-domaines (Terre, Air, Espace, Mer, Cyber) et multi-champ (physique, EM, EO, IR)
- Elaboration de la situation tactique

- Compréhension et anticipation des manœuvres ennemies
- Elaboration des manœuvres amies
- Planification des ordres, production
- Exécution les plans de batailles, évaluation, correction

Dans la suite du document, le terme C2 désignera le SI (Système d'Information) C2.

Le C2 couvre l'ensemble du cycle de la bataille (planifier-préparer-conduire-évaluer), mais reste distinct du système d'armes. Le C2, selon l'échelon auquel il se situe, doit répondre ou pas à des contraintes de temps réel (garantie de temps d'exécution, en valeur et/ou en écart-type).

2. Comment évolue la guerre?

La manière de faire la guerre évolue depuis 2010 (et en particulier l'Afghanistan), et singulièrement depuis le conflit en Ukraine, avec les caractéristiques suivantes :

- La complexité qui se traduit par la nouvelle approche M2MC (Multi-Milieus Multi Champs) ou son équivalent NATO MDO (Multi Domain Operations)
- La transparence du champ de bataille qui lève le brouillard de la guerre et rapproche la situation réelle de la situation perçue.
- L'accélération du tempo, le raccourcissement des boucles OODA (*Observe, Orient, Decide, Act*)
- La robotisation (dont les drones), et la prolifération des acteurs dans la 3D

Dans ce combat de haute intensité, il est crucial d'arbitrer rapidement et intelligemment entre l'emploi d'effecteurs en masse et à bas coûts et d'effecteurs de haute technologie, pour réserver l'emploi de ces derniers à la neutralisation de cibles stratégiques ou la protection d'unités à haute valeur.

Face à ces nouvelles tendances du champ de bataille, la charge cognitive du soldat augmente significativement. Motoriser les C2 avec de l'IA est nécessaire pour permettre aux unités de conserver la supériorité sur l'ennemi.

3. Qu'est-ce que l'IA pour les C2 ?

Traditionnellement, on distingue l'IA des modèles de l'IA des données même si ces deux approches tendent à se rapprocher pour former l'IA hybride.

L'IA des modèles est une informatisation de la connaissance humaine. Typiquement, les systèmes à base de règles (comme les systèmes experts) relèvent de cette catégorie. L'expertise humaine est modélisée. L'IA des modèles s'apparente ainsi à de l'algorithmie un peu particulière. Elle est particulièrement adaptée aux problématiques que l'on sait mal modéliser de façon déterministe.

L'IA des données fait l'hypothèse que la connaissance est intrinsèquement contenue dans les données.

L'apprentissage machine consiste pour l'IA des modèles à les préciser / compléter par l'ajout de nouvelles connaissances et pour l'IA des données à mieux les classer / associer par l'annotation par des experts le plus souvent humains (apprentissage supervisé) ou par analyse automatique (apprentissage non-supervisé). Pour les IA génératives, on parle d'apprentissage auto-supervisé parce qu'elles apprennent en visant à « deviner » les éléments qu'elles ont elles-mêmes extraits de séquences complètes (typiquement, pour le texte, elles cherchent à « deviner » le mot complétant une phrase dont elles ont extrait un ou plusieurs mots et qu'elles connaissent donc par construction).

L'apprentissage par renforcement consiste (pour les deux formes d'IA, modèle et donnée) à améliorer les performances par l'expérience (essais / erreurs) éventuellement supervisée, une fonction dite d'évaluation permettant de comparer les performances relatives de deux solutions potentielles. La programmation génétique est une forme particulière d'apprentissage dans laquelle des populations de solutions potentielles à un problème sont manipulées suivant les principes de l'évolution darwinienne (croisements, mutation, sélection...).

L'hybridation des différentes formes d'IA (majoritairement à base d'apprentissage) semble la plus efficace. Cette IA hybride permet de bénéficier des avantages relatifs des deux approches (performance, interprétabilité...). En généralisant, l'approche hybride associe également d'autres types de connaissances (mathématiques, physiques...).

Comparée à une analyse purement humaine, l'IA permet de traiter d'immenses volumes de données en temps réel,

ce qui dépasse largement la capacité humaine. Quand bien même on « alignerait » un grand nombre d'analystes humains pour effectuer un travail similaire, les échanges nécessaires entre eux pour converger sur une analyse commune rendrait l'exercice inefficace. Une IA basée sur de l'apprentissage permet potentiellement d'améliorer ses performances au cours du temps contrairement à des algorithmes traditionnels. Une IA correctement définie et déployée permet, par ailleurs, de repérer des motifs subtils dans les données que les méthodes classiques ne détectent pas. Les données traitées pouvant être de différentes natures : texte, images, vidéos, sons, radar, sonar. L'IA peut interpréter des données complexes et floues que les approches statistiques classiques ont du mal à modéliser.

4. Quels sont les bénéfices de l'IA dans les C2 ?

Les bénéfices pour les opérationnels utilisateurs des C2 sont multiples :

- Rapidité et qualité de l'aide à la décision, pour permettre de prendre l'ascendant sur ENI :
 - Traitement massif de données pour une meilleure compréhension de la situation et des menaces
 - Proposition de scénario d'actions
 - Orchestration de la manœuvre
- Automatisation de processus ancillaires et souvent manuels, permettant de libérer du temps, alléger la charge cognitive des soldats.
- Nouvelles capacités, par exemple de lutte anti FPV que permet un raccourcissement suffisant de la boucle OODA (senseur – C2 – effecteur).
- Cybersécurité par détection d'intrusion ou de comportement malveillant.

5. Quels sont les services rendus par un C2 motorisé à l'IA ?

Les exemples contenus dans ce chapitre sont essentiellement issus du domaine Terre.

5.1 Elaboration de la situation tactique

Une situation tactique (SITAC) complète et à jour est la base de la prise de décision. La SITAC se construit à partir des détections effectuées par les capteurs et l'échange d'information entre les acteurs.

La principale difficulté réside dans la fusion d'informations provenant de sources et de formats variés, incomplètes, imprécises en temps et en position, accompagnées ou non de métrique d'incertitude. La SITAC reposant sur l'échange d'informations entre les acteurs, elle est tributaire du caractère DDIL (*denied, degraded, intermittent, limited*) des communications. Des chaînes de traitement hybrident plusieurs technologies pour construire la SITAC, et l'opérateur humain doit pouvoir réaliser des actions correctrices sur la SITAC, telles que regrouper deux pistes en une seule (ou inversement séparer), modifier le type d'unités détectées, etc. La performance du processus de maintien de la SITAC et des trajectoires (Figure 1) nécessite la combinaison de l'expertise technique et métier.



La seconde difficulté est de présenter une SITAC suffisamment synthétique pour permettre une prise de décision rapide. Des analyses utilisant des techniques d'IA et la doctrine ennemie permettent de proposer des visualisations avec un premier niveau de synthèse, grâce au regroupement d'unités ENI, la caractérisation de la formation de l'unité et même des propositions de missions ENI. Ainsi, la construction de la SITAC est augmentée par des moyens de visualisation et de navigation pour permettre à l'utilisateur d'accéder au juste niveau d'informations pour sa prise de décision.

Figure 2- Reconstitution de trajectoire

D'un point de vue pratique, Thales développe une chaîne de traitement ("Agent Data Analysis Pipeline") pour l'analyse sémantique automatique de la situation tactique, optimisant la prise de décision opérationnelle dans des environnements complexes à observabilité partielle. En exploitant des données issues de multiples capteurs (optique, radar, acoustique), cette chaîne assure la détection et la classification probabiliste d'entités, leur fusion en pistes cohérentes et leur regroupement (clustering), conformément à une base de connaissances contextuelle préalablement modélisée. Par exemple, sur la **Figure 1**, différents pions de type char ont été regroupés dans des entités peloton (en l'occurrence 3 pelotons).

L'architecture modulaire de cette chaîne de traitement



Figure 1 – Reconstitution d'ordres de bataille

repose sur trois niveaux distincts.

- 1) Traitement multi-capteurs, détection et pistage, qui permettent dans notre exemple de détecter les chars
- 2) Analyse descriptive, partitionnement et classification des groupes d'entités, surveillance d'événements tactiques. Cette étape permet de déduire les pelotons, de les suivre même quand le réseau de capteurs les perd, de caractériser l'échelonnement des pelotons.
- 3) Raisonnement, inférence des intentions et estimation des zones d'intérêt. Cette étape permet d'inférer des intentions probables de l'ennemi. On cherche ici à répondre aux questions qui se posent lors de la MEDOT.

En s'appuyant sur des techniques avancées (partitionnement hiérarchique agglomératif et basé sur les graphes, filtre de Kalman adaptatif et raisonnement bayésien), la solution transforme des données brutes hétérogènes en une synthèse claire de la situation tactique. Ainsi, elle facilite la compréhension des dynamiques opérationnelles, anticipe les mouvements adverses et optimise l'emploi des moyens de renseignement (essais de drones notamment), garantissant un avantage stratégique dans des champs

de bataille semi-transparents et hautement dynamiques.

Pour accompagner un processus davantage amont tel que le processus OTAN CCIR (Commander's Critical Information Requirements), l'IA Thales permet de manipuler une grande masse de données hétérogènes sur un temps long et de comprendre ainsi la menace stratégique et son évolution (figure 3). Elle décèle des patterns d'activités MDO et offre ainsi des capacités d'anticipation des menaces pour s'y préparer.

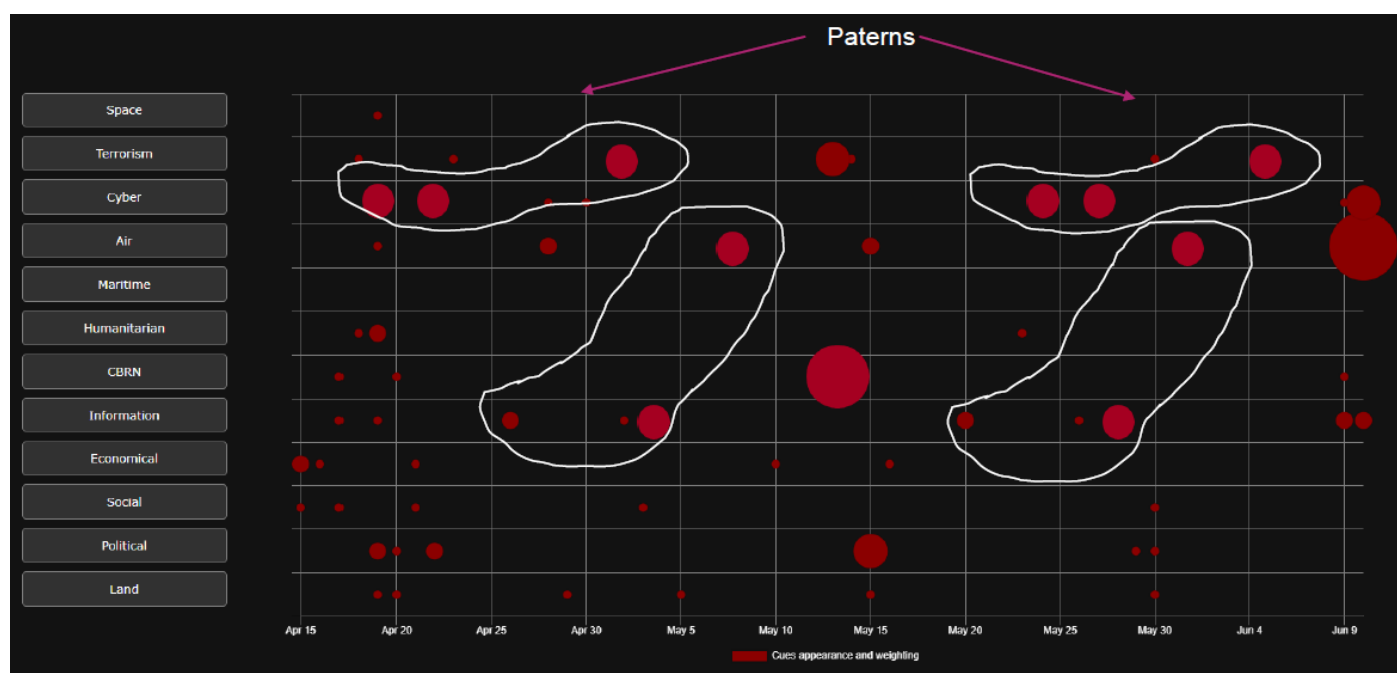


Figure 3 – Détection de patterns d'activités pour anticiper des menaces

5.2 Proposition de manœuvre AMI / ENI

Sitôt la SITAC établie et quelques intentions ennemies identifiées, l'IA Thales propose une riposte qui peut prendre la forme d'un FragO (Fragmentary Order) détaillant des ajustements tactiques immédiats, ou d'un Overlay Order qui superpose graphiquement les plans d'action sur une carte opérationnelle pour une visualisation claire par les unités.

L'IA Thales agrège des sources de données diverses (MNT, bitmap, routes, voies ferrées), et génère (figure 4)

- Une carte 2D de « mobilité » par unité. Chaque pixel a une couleur, qui indique une mobilité plus ou moins facile. Cette carte est construite à partir

d'abaque : pour la Cavalerie, il faut des routes de telle largeur par exemple

- Les zones de combat, favorable à l'affrontement : la forêt est favorable à l'infanterie, mais pas à la cavalerie

5.3 Planification, aide à la décision, rédaction des ordres

Au cœur de l'aide à la décision se trouve la problématique du choix d'une solution parmi plusieurs, sur la base d'un ensemble de critères en conflits dans le sens où il

Figure 4 – Segmentation sémantique et compression

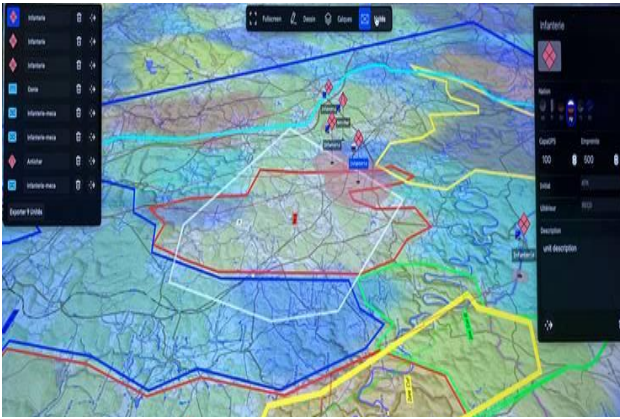


Figure 5 – Carte de mobilité



n'existe pas une solution qui est la meilleure sur tous les critères. Par exemple, on peut considérer l'allocation de drones pour identifier des menaces qui ont été détectées. On peut envoyer beaucoup de drones pour réduire les délais, mais au détriment de la capacité à traiter une menace prioritaire future qui pourrait être détectée. Une fois les critères de décision identifiés, il faut spécifier les compromis les plus acceptables entre ces critères pour le décideur. Conserver 2 drones (pour des menaces futures) ou réduire la durée de la mission de 30mn ? L'outil MYRIAD Thales aide à construire un modèle de préférence multicritère, fidèle à l'expertise, capable de représenter des interactions entre critères et d'expliquer les décisions sous forme de scores d'influence des critères sur l'évaluation globale. Cet outil a été utilisé lors d'un exercice REPMUS 24 pour la planification des drones.

5.4 Services techniques

Afin d'assurer la qualité des services proposés à ses utilisateurs, un C2 s'appuie sur des services techniques parfois complexes dont certains peuvent bénéficier de l'IA. Par exemple :

- Création et maintenance des passerelles d'interopérabilité afin de traduire les messages communiqués dans le cadre d'opérations multi-domaines ou en fédération, c'est-à-dire entre des acteurs qui utilisent des modèles de données différents. Sans l'automatiser entièrement, les assistants IA pour le traitement des spécifications et le codage logiciel permettent de réduire le temps de mise à jour des passerelles tout en

nécessitant un niveau de technicité moindre de la part des opérateurs.

- Ajustement du niveau de compression des données à transmettre selon les contraintes des ressources calcul-mémoire-réseau. Lorsqu'elle est possible, l'implantation d'IA côté émetteur permet une compression plus ou moins agressive des données complexes pour réduire la consommation de la bande passante avant une reconstruction côté réception dont la fidélité peut être choisie selon la criticité de l'information.

La figure 5 ci-dessus présente un résultat obtenu sur



une plateforme mobile (type NVIDIA Jetson). En haut à gauche l'image d'origine, en haut à droite une segmentation sémantique avant envoi, en bas on compresse fortement les masques sémantiques et on conserve les pixels des régions d'intérêts. En bas à gauche, on conserve les voitures ; en bas à droite les voitures, personnes et bâtiments sont peu compressés, le reste est fortement compressé.

Entre les deux images du haut, on compresse d'un facteur 100.

- Exploitation des journaux techniques d'un ensemble de sous-systèmes hétérogènes à la recherche de causes racines. L'usage d'assistants IA simplifie et accélère la fouille des données en interprétant des requêtes faites directement en langue naturelle, en utilisant les connaissances et procédures issues des manuels techniques disponibles et en corrélant les informations issues

de plusieurs sources différentes, afin de faire gagner du temps aux techniciens sur des tâches longues et fastidieuses pour se concentrer sur la tâche d'analyse à haute valeur ajoutée.

6. Principes d'architecture des C2 motorisés à l'IA

Un C2 motorisé à l'IA s'architecture différemment et développe des nouvelles fonctions.

- L'exploitation de données massives hétérogènes requière une architecture qui optimise les performances d'accès aux moyens de stockage et de calcul en supprimant les interfaces inutiles et les couches de virtualisation.
- L'accès aux données doit être sécurisé avec des mécanismes de protection classiques (gestion des droits, chiffage des flux, ...), des politiques ABAC (Attribute Based Access Control) aux standards DCS (Data Centric Security) pour l'échange de données entre systèmes.
- Le C2 motorisé à l'IA doit offrir des outils basés sur des standards ouverts pour faire cohabiter des applications qui utilisent des technologies différentes, administrer et superviser les ressources entre les différents utilisateurs et les différentes applications tout en garantissant la résilience globale et la sécurité d'accès aux données.
- Les modèles d'IA doivent être mise à jour régulièrement, le C2 doit donc inclure un atelier MLOps (Machine Learning Operations), utilisable en métropole ou sur le théâtre, pour permettre la préparation de nouvelles données d'entraînement et des tests, leur annotation, l'entraînement des modèles IA avec ces nouvelles données, la vérification de la performance des modèles mis à jour, puis le déploiement.
- L'interface homme machine doit permettre d'interroger en langage naturel (« préviens-moi si les unités ennemies manœuvrent »), déclencher un agent IA qui scanne les sources d'informations disponibles, analyser le contenu et envoyer les alertes en temps réel à l'utilisateur. Le C2 doit donc être architecturé avec un framework technique disposant d'agents IA dédiés aux différents métiers du C2.

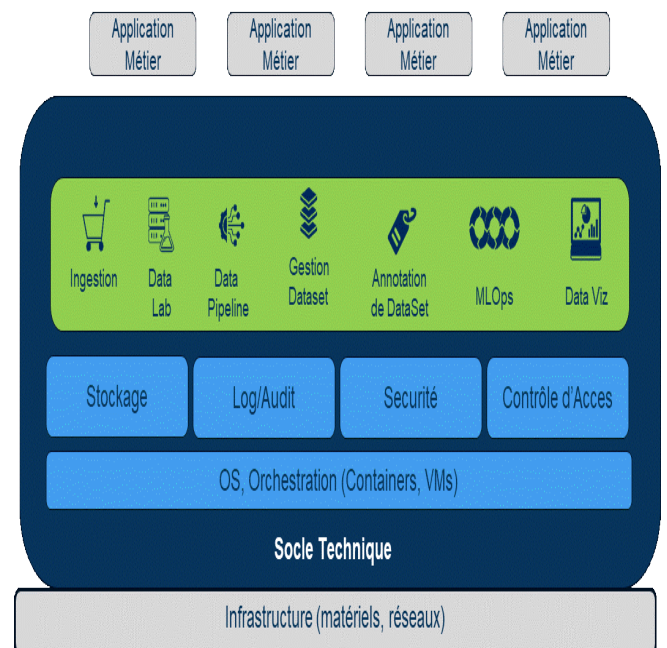
- Enfin les modèles d'IA doivent expliquer les sources utilisées pour produire la décision, décrire l'arbre de décision et présenter un score de confiance fiable du résultat

En conséquence, l'architecture du C2 motorisé à l'IA se présente ainsi :

- L'OS directement posé sur l'infrastructure, l'orchestrateur de containers et de VMs qui assure à la fois la scalabilité et la résilience du système.
- Les services techniques de stockage, de sécurité et de contrôle d'accès aux données (RBAC, ABAC, DCS)
- Les services dédiés à l'IA et la gestion des données : ingestion et préparation des données hétérogènes en stream et en batch, data lineage (processus qui permet de visualiser et suivre le cycle de vie des données, en détaillant les transformations, traitements et réutilisations), Data Lab pour l'exploration des données, Data Viz pour la visualisation des données, atelier MLOps.

7. Les défis de l'IA dans les C2 et les réponses associées

Ce chapitre décrit les multiples défis que pose l'introduction de l'IA dans les C2, et les réponses que Thales apporte.



7.1 Manque de données

Dans le contexte militaire, l'accès aux données en grande quantité est souvent difficile, à cause de la confidentialité de ces données, le faible nombre de certains équipements ou leur faible durée de vie (munitions). Autant les systèmes experts et arbres de décision sont peu gourmands en données, autant l'apprentissage profond (deep learning) et les modèles de fondation sont très consommateurs.

La réponse que Thales apporte à cet enjeu de manque de données d'entraînement est multiple :

- L'utilisation de petits modèles moins expressifs (l'expressivité d'une IA représente l'ensemble des fonctions que le modèle peut représenter), de jeux de données de pré-entraînements ou bien de parties de modèles déjà entraînés
- Des simulations physiques, des générations de données simulées ou de données hybrides par diffusion, qui permettent de produire de larges jeux de données d'entraînements.
- Des modèles de fondation sur des senseurs spécifiques sont en cours de développement. C'est le cas des images satellitaires.
- Les modèles à espace latent structuré en distance ou les modèles hybrides à composante non-IA ou à composante physique sont prometteurs.

7.2 Vulnérabilité

Il s'agit de se protéger contre le leurrage de l'IA d'origine malveillante ou, réciproquement, de tenter de leurrer les IA ENI. Leurrer l'IA peut se réaliser de 2 manières :

- Exploiter les biais de l'IA en cherchant et utilisant les faiblesses du module d'IA proprement dit ou des processus construits autour de cette IA
- Créer des biais dans l'IA en amont de son déploiement

Illustrons la première manière de leurrer l'IA par un exemple dans un processus C2 de ciblage. L'ENI fait du ciblage sur des unités AMI à haute valeur dans la profondeur, sur la base de renseignements (ELINT, IMINT, OSINT), il dispose pour cela d'un outil de fusion des flux des capteurs et d'IA d'aide à la décision pour une accélération de la boucle Feu. Ses cibles prioritaires sont les PC de division, les radars de contre-batterie, l'artillerie longue portée, les dépôts de munitions et de carburant.

L'effet recherché AMI est de protéger ses unités à haute valeur et de consommer les moyens ENI sur des fausses cibles, en leurrant l'ENI selon les moyens suivants :

- Détournement de l'IA ENI de fusion et d'aide à la décision
- Appâts numériques par injection dans les flux adverses de données de renseignement biaisées (réseaux sociaux, bases ELINT / IMINT, documents récupérés ou signaux captés)
- Création d'unités factices telles que structures gonflables réalistes, simulateurs thermiques, émetteurs EM, robotique passive.

Pour améliorer la robustesse des d'IA dans les systèmes C2 face aux menaces et moyens précitées, Thales a structuré une équipe cortAlx de « Friendly Hackers », qui intervient en phase de conception d'un système et en aval pour faire l'analyse d'une solution existante.

La librairie BattleBox développée par cette équipe, utilisable durant la phase d'ingénierie du C2, rassemble des outils d'attaques et de défenses spécifiques à l'IA, tel qu'un détecteur de deepfakes images et voix, un détecteur de portes dérobées dans un modèle. Pour tester un modèle avant son déploiement, elle propose une collection d'attaques permettant de faire des tests rapides de robustesse d'un modèle face aux exemples antagonistes et face aux requêtes visant l'extraction des informations sensibles. Les Friendly Hackers peuvent ainsi mener des missions de pentest sophistiquées.

Dans l'exemple précédent, la BattleBox des Friendly hackers pourra être utilisée pour les 2 premiers points.

7.3 MLOps

Le C2 motorisé à l'IA modifie le processus de MCO (Maintenance en Condition Opérationnel). Les modèles d'IA doivent être mis à jour lorsque l'environnement, les équipements ou les comportements du champ de

bataille évoluent. L'Ukraine nous enseigne que la rapidité des évolutions sur le théâtre est incompatible avec le modèle classique de demande d'évolution puis modification des modèles en usine puis livraison d'une nouvelle version. L'atelier MLOps répond à cet enjeu. Une chaîne MLOps est un ensemble d'outils et de technologies intégrées destinés à simplifier et accélérer la séquence d'opérations qui transforme des données en un modèle ML.

Une chaîne MLOps apporte ainsi les bénéfices suivants :

- Automatiser les tâches coûteuses et complexes
- Faciliter le développement sur des environnements avec différents niveaux de sécurité
- Fournir et créer de l'AI éthique, explicable et fiable.
- Supporter les produits ML à travers leur cycle de vie entier

4 rôles sont nécessaires pour exécuter cette séquence d'opérations

- Le data scientist qui prépare, explore, transforme, labélise, et versionne les données
- L'expert cyber qui va détecter les empoisonnements des données
- Le modèle scientifique qui entraîne le modèle
- L'expert utilisateur qui évalue la performance opérationnelle de la fonction C2 motorisée à l'IA

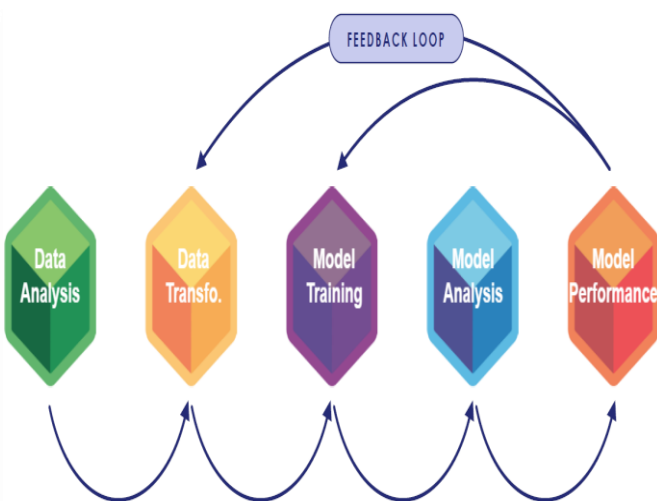


Figure 8 – Principes d'une chaîne MLOps

Réaliser le processus MLOps en Métropole permet de mutualiser les expertises scientifiques, mais qui sont alors éloignés des utilisateurs. Le réaliser sur le théâtre nécessite des infrastructures type Data Hub et des compétences. La meilleure solution dépendra sans doute de la taille du théâtre, il est donc nécessaire de

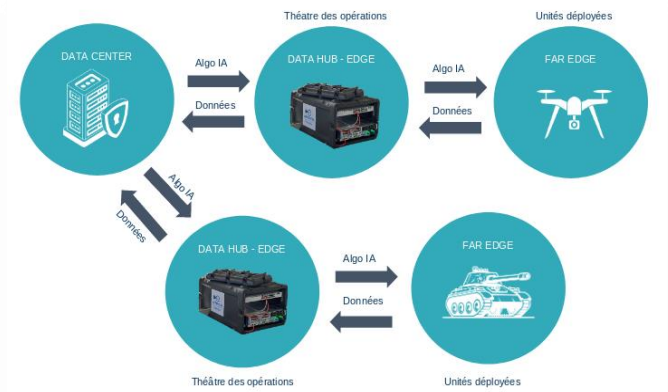


Figure 7 - Adaptabilité de la solution en fonction du déploiement

construire une solution qui s'adapte aux contraintes opérationnelles et au déploiement :

- Un modèle réalisé en Métropole peut être déployé sur différents théâtres et jusqu'à des objets situés en Far Edge
- Un modèle mis au point sur le théâtre peut aussi être déployé en Far Edge.
- Le modèle mis au point sur le théâtre sera aussi retransmis en Métropole afin d'être déployé sur d'autre Data Hub en théâtre

7.4 Cyber sécurité

Comme tout SI, un SI C2 motorisé à l'IA doit faire l'objet d'une décision d'homologation, qui nécessite une démarche rigoureuse : définition du SI (fonctions, emploi, architecture, procédures de maintenance), analyse de risques, définition des mesures de sécurité et identification des risques résiduels.

Or, le monde de l'Intelligence Artificielle se caractérise par des évolutions technologiques très rapides et l'apparition continue de nouveaux composants et applications, couplée à un travail en continu sur les données de production de façon à maintenir la fiabilité des algorithmes. Ces exigences, qui façonnent l'architecture du C2 comme nous l'avons vu §5, imposent des contraintes de sécurité particulières.

En outre, le processus d'homologation du MoD devra nécessairement s'adapter pour tenir compte de la spécificité des SI C2 motorisés à l'IA, en particulier l'introduction du MLOps.

7.5 SWaP (Size, Weight and Power)

Les Forces traitent les données au plus près du théâtre, là où les contraintes d'encombrement et de puissance sont fortes. Or, autant les systèmes experts et les arbres de décision sont peu gourmands, autant les réseaux de neurones ou les LLMs le sont.

Les plateformes étant très diversifiées en termes de SWaP, les solutions ne sont pas universelles, et rejoignent celles évoquées au §6.1. Actuellement, elles mettent en œuvre des IA peu gourmandes (ex. system experts ou arbre de décision) ou bien des petits modèles d'IA sur FPGA ou sur des petits GPU. Une pratique répandue, notamment pour les drones, est de remplacer un seul grand modèle par une bibliothèque de petits modèles moins gourmands et d'en changer en fonction des conditions de vols (résolution au sol, définition capteur, ...) ou des types de mission. D'autres solutions vont émerger rapidement, ceci grâce aux recherches du secteur civil sur les robots autonomes, sur les assistants personnels et sur le développement des SLM (small language models).

7.6 Confiance, Qualification

L'intégration de l'IA dans les systèmes C2 impose de repenser fondamentalement les approches traditionnelles de qualification et de certification. La confiance dans ces systèmes ne peut plus reposer uniquement sur des vérifications traditionnelles de logiciels déterministes. Elle doit intégrer la nature probabiliste et évolutive de l'IA, où les décisions émergent de processus d'apprentissage continus et de réseaux de neurones dont la logique interne reste partiellement opaque.

Or, prouver qu'on peut faire confiance à l'IA est fondamental, sinon elle sera rejetée par l'utilisateur.

Les attributs de la confiance liés à l'IA concernent en particulier :

- L'explicabilité et la transparence : les utilisateurs doivent pouvoir comprendre, au moins partiellement, comment le système parvient à ses conclusions. L'IA n'a actuellement pas de bon sens, avec le risque de ne pas s'apercevoir que sa réponse est absurde.
- La reproductibilité : l'IA est basée sur des fonctions non-linéaires, et pourrait donner une réponse très

différente à une situation très proche. Une IA doit produire la même conclusion avec des données d'entrée similaires.

- La robustesse : Le C2 motorisé à l'IA doit être capable de détecter une attaque sur les données, tel que nous l'avons vu au §7.2.
- La surveillance : une IA de confiance doit savoir estimer la précision de sa conclusion (score de confiance). Plus généralement, une métrologie propre à l'IA est mise en œuvre pour s'assurer que l'IA se comporte correctement durant son exécution. Thales développe ses propres outils, par l'exemple l'algorithme SCIO (*Statistical Confidence from Internal Observations*) disponible sur GitHub.

Prouver qu'on peut faire confiance à l'AI est un challenge scientifique qu'aide à relever le projet Confiance.ai, dont l'objectif est de fournir des méthodes et outils destinées à garantir et prouver le bon fonctionnement de l'AI, en adaptant les pratiques d'ingénieries système, logiciel. La chaîne MLOps Thales telle que décrite au §7.3 intègre d'ores et déjà des composants confiance.ai.

Pour davantage de détails, le lecteur pourra se référer au white paper Thales « *Le cycle de vie de l'ingénierie de l'IA de confiance pour les systèmes critiques* »

Thales poursuit sa R&D, en particulier dans l'élaboration de scores de confiance. Une IA produit toujours un résultat et un score de confiance associé. Pour une IA qui n'a été entraîné qu'avec des images de chats et chiens, si on lui présente un éléphant en entrée, la fonction SoftMax en sortie du réseau produira un résultat « chat » avec un score de confiance de 0,8 et « chien » à 0,2. Le bon score de confiance présentée par l'IA aurait dû être 0 puisque l'IA n'a jamais eu d'éléphant dans ses données d'entraînement, mais l'IA ne sait pas qu'elle ne sait pas. Thales travaille sur une méthode qui établit un score de confiance liée à la distance entre la donnée d'entrée et le dataset d'entraînement, dans le cadre de règles, telles que la nécessité d'établir un score de confiance sans connaître le dataset d'entraînement. En fonction du cadre d'emploi opérationnel, la méthode Thales en déduit des règles, puis une combinaison de méthodes de scoring pour obtenir un score de confiance le plus juste possible.

7.7 Charge cognitive

L'IA dans les C2 permet d'accélérer le cycle de décision OODA. Mais l'homme dans la boucle reste essentiel, l'IA propose et le soldat dispose. Le défi est donc une surcharge cognitive du soldat, submergé par les analyses et propositions de l'IA sur un rythme accéléré de la guerre.

Comment donc organiser au mieux cette collaboration entre IA et soldat et la rendre adaptable ?

L'utilisation de la méthode STPA (System-Theoretic Process Analysis) lors de l'ingénierie du C2 apporte une partie de la solution. Cette méthode d'analyse de risques permet d'identifier - au sein de processus dans lesquels des SI, des machines et des hommes interagissent - les moments à risques, en particulier à risque léthal. La méthode permet de mettre en exergue là et quand cela pourrait mal se passer, puis propose des contre-mesures, des exigences de conception, des checks list pour les acteurs. Cette méthode a été utilisée lors du challenge CoHoMa organisé par le Battle Lab Terre du Ministère des Armées.

Cette méthode sera d'autant plus efficace qu'elle pourra être alimentée d'une mesure (via un dispositif de type BCI Brain Computer Interface) ou d'une estimation (via une IA d'analyse comportementale) de l'état du soldat (stress, charge cognitive).

7.8 Adoption par les utilisateurs

Pour qu'un C2 motorisé à l'IA soit accepté et adopté par les opérationnels, plusieurs conditions doivent être réunies, tant sur le plan technique qu'humain.

- Le chef doit rester maître du tempo et de la décision. L'IA propose, l'humain dispose. Toute recommandation issue de l'IA doit être compréhensible, traçable, justifiable. Les arbres de décision, scores de confiance et données sources doivent être accessibles au commandant.
- Le C2 IA doit préserver la chaîne hiérarchique. Le principe de subsidiarité reste un pilier fondamental du commandement français. L'IA ne doit pas court-circuiter les niveaux N+1 ou N-1 au nom de la vitesse, mais renforcer leur efficacité grâce à une diffusion maîtrisée et contextualisée de l'information.
- L'IA doit soulager, non alourdir. Elle libère du temps et de l'attention pour les tâches à haute valeur ajoutée. Cela suppose une ingénierie fine

des interfaces et des flux, adaptée aux contraintes opérationnelles.

Plusieurs travaux en cours (DGA, ONERA, OTAN CWIX et SCORPION) visent à développer des modèles de confiance calibrée, capables d'alerter lorsqu'un opérateur se désengage excessivement ou délègue sans discernement. Certains prototypes explorent même l'estimation en temps réel de la confiance implicite, à partir d'interactions ou de données physiologiques. Ces approches, encore exploratoires, visent un objectif commun : maintenir l'humain dans la boucle, sans le saturer, sans l'aveugler.

Après le trop peu de confiance, l'enjeu suivant sera la trop grande confiance. L'IA ne doit pas chercher à séduire, mais à informer. Une machine parle comme une machine, et doit être perçue comme telle. Les opérationnels n'attendent pas un agent intelligent qui interagit, mais un assistant spécialisé, discret, efficace, qui reste à sa place. L'IA se cache derrière un bouton, produit une synthèse, filtre l'information, allège la charge mentale — mais ne pense pas la tactique, ne prend pas l'initiative, et ne simule pas l'intuition humaine. L'IA ne doit pas réduire le chef militaire à un opérateur technique. Elle doit renforcer sa capacité d'action, en valorisant ses compétences spécifiques : discernement stratégique, intuition tactique, responsabilité morale. Cela suppose une acculturation ciblée aux IA de commandement, non pour les maîtriser techniquement, mais pour les superviser lucidement.

L'acceptation repose sur la transparence, la simplicité, et la possibilité de reprendre la main à tout moment. L'IA ne doit pas être une boîte noire, ni un fantôme algorithmique, mais un outil militaire intégré, explicable, robuste et maîtrisé. L'adoption réussie d'un C2 motorisé à l'IA ne dépend pas seulement de ses performances technologiques, mais de sa capacité à renforcer la mission du chef militaire, en lui redonnant l'espace pour décider, manœuvrer, et conserver l'ascendant dans la complexité croissante des engagements modernes.

8. À propos de Thales

Thales est exposé aux sujets présentés dans ce document à travers ses diverses activités commerciales. Depuis près d’une décennie, l’IA est intégrée dans son portefeuille de produits, en particulier dans des solutions critiques et de défense déjà vendues ou destinées à être vendues dans plusieurs pays à travers le monde. Cette expérience a permis aux équipes de recherche et d’ingénierie de Thales de développer des composants, outils et méthodologies d’IA pour concevoir des systèmes performants intégrant l’IA et faciliter l’usage de l’IA dans des environnements souverains et internationaux. Thales compte plus de 800 experts en IA. Ces experts font désormais partie de l’organisation interne cortAlx créée en 2024. Ils sont répartis entre les équipes Labs, Factory et Sensors, qui développent ensemble les modèles, les chaînes d’outils, la cybersécurité, les éléments d’infrastructures critiques et l’intégration dans des systèmes plus larges, autant d’aspects nécessaires pour rendre l’IA pleinement opérationnelle. Ils sont situés en France, au Royaume-Uni, au Canada, à Singapour et aux Émirats arabes unis.





4, rue de la Verrerie 92190
Meudon FRANCE

Tél. + 33(0)1 57 77 80 00

www.thalesgroup.com

