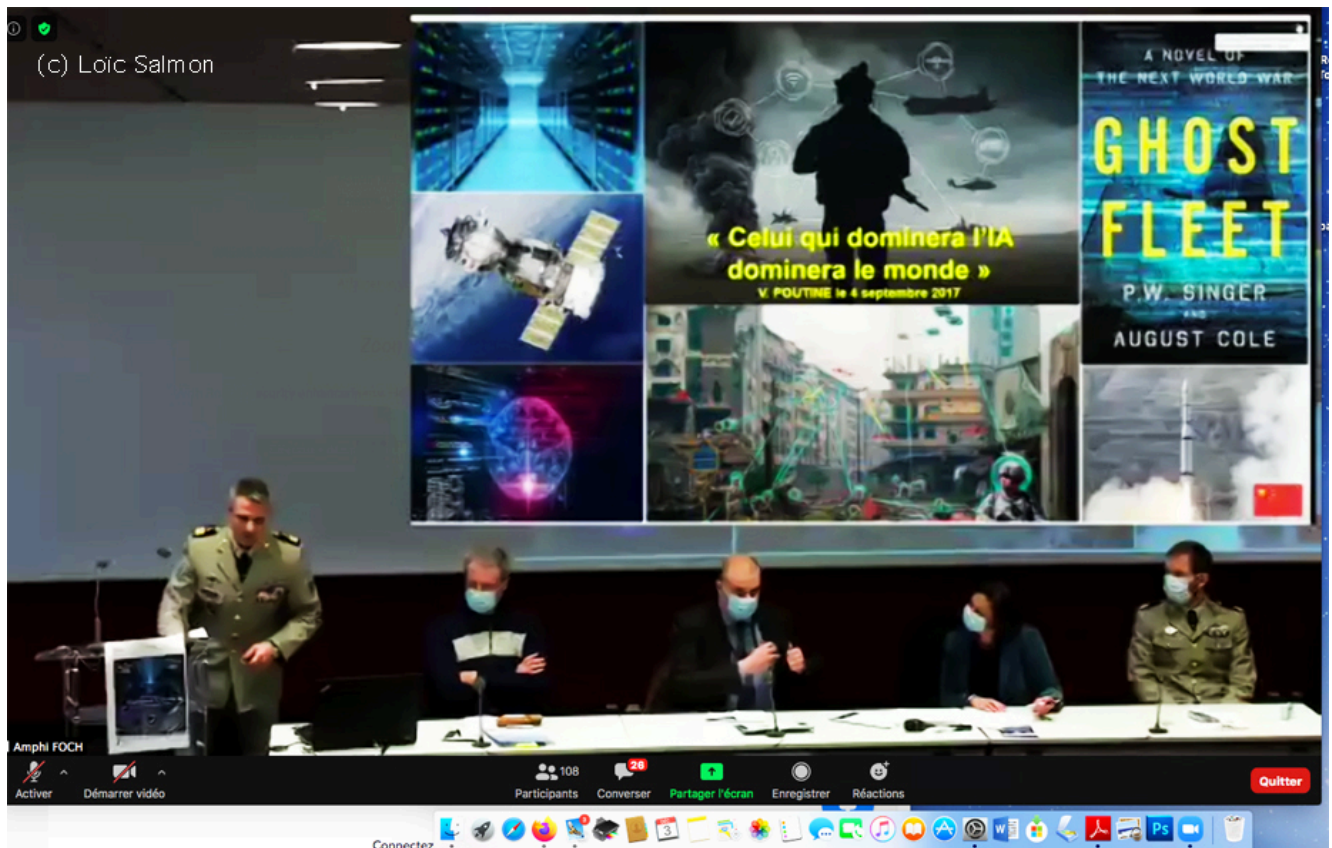


Défense : l'IA dans le champ de bataille, confiance et contrôle



Sur le plan militaire, l'intelligence artificielle (IA) devra traiter des données caractérisées par leurs volume, variété et véracité. Outre son efficacité technique, elle doit inspirer confiance à son utilisateur, qui prend la décision.

Ce thème a fait l'objet d'un colloque organisé en visioconférence, le 3 décembre 2020 à Paris, par le Centre de recherche des Ecoles de Saint-Cyr Coëtquidan (CREC). Y sont notamment intervenus : le colonel Christophe Augustin, officier de cohérence opérationnelle à l'Etat-major des armées ; Jean-Michel Tran, directeur technique chez Naval Group ; Aurélien Strippoli, directeur de l'innovation chez Airbus Defence & Space ; l'ingénieur général de l'armement Jérôme Lemaire chargé de mission IA à la Direction générale de l'armement. Julien Nocetti, enseignant-chercheur au CREC.

Contraintes spécifiques. Depuis la fin de la guerre froide (1991), le contexte stratégique est devenu plus complexe, imprévisible et dynamique, rappelle le colonel Augustin. La confrontation possible avec des Etats puissances et des acteurs non étatiques apparaît avec la fin de la supériorité technologique

occidentale et la facilité d'accès aux technologies de rupture. L'interopérabilité interalliée s'impose, car aucun pays n'aura la capacité de répondre seul à un conflit de grande ampleur. Ce conflit pourrait débuter par des opérations hybrides dans les domaines terrestre, aérien, maritime, cyber, informationnel et spatial. L'IA permettra de détecter les signaux faibles avant-coureurs d'une crise. Les forces déployées sur un théâtre d'opérations devront anticiper les phases de silence radio et les pertes du lien satellitaire, de la supériorité électronique ou de la supériorité aérienne. Le ministère des Armées va disposer des trois « clouds » informatiques d'ici une quinzaine d'années. Le premier, dit « cloud central » ou modèle d'accès à un pool partagé de ressources informatiques à la demande, nécessitera la disponibilité de réseaux interopérables mondiaux à haute capacité, dont la téléphonie mobile 5 G. Le déploiement de forces sur un théâtre d'opération extérieur nécessitera la constitution d'une zone d'autonomie par un « cloud d'entrée de théâtre » et un « cloud de combat », modèles d'accès aux services de métiers spécifiques (plates-formes d'armes, fonctions commandement et contrôle adaptatives etc.). Ils nécessiteront la disponibilité de réseaux de missions fédérées et sécurisées. Les armées ont besoin de capacités de pointe et souveraines. Les outils de demain devront surtout être simples à déployer, à utiliser et à administrer.

Usages navals. Une force navale regroupe des systèmes de systèmes, explique Jean-Michel Tran. Le maintien de la supériorité navale résulte de la réussite de la transformation numérique du combat naval, Système très complexe qui doit durer plusieurs mois dans un environnement marin difficile et sur un théâtre d'opération hostile, un navire doit rester en alerte permanente et capable de répondre instantanément à une menace venant de n'importe où. Par exemple, la réaction à une attaque de type missile hypervélocité est de l'ordre de quelques secondes. Outre une vision élargie des enjeux du théâtre d'opération et une connaissance précise de l'état opérationnel du navire, l'équipage doit disposer d'une aide à la décision synthétique, pour limiter les erreurs dues au stress ou à la fatigue. L'IA permet déjà la détection des pannes/alertes pour la propulsion des frégates multi-missions, grâce à une maintenance prédictive. Elle développera l'autonomie de décision des drones marins, afin d'augmenter leurs performances en précision, vitesse et sécurité. Un algorithme à multicritères calculera les plans d'engagement par la veille coopérative, l'évaluation de la menace, la coordination des engagements, la mise en œuvre des armes et l'évaluation de l'interception. Ainsi pour la protection du groupe aéronaval, une frégate d'escorte détectera la

menace d'un missile supersonique, le poursuivra et le désignera comme objectif à une autre frégate d'escorte, qui le neutralisera. L'IA aura proposé à l'officier de lutte anti-aérienne la meilleure solution en temps réel. Elle aura choisi les armes, optimisé l'efficacité, géré les stocks de munitions, évité le sur-engagement et minimisé la gêne pour la force navale.

Domaine aérien. Selon Aurélien Strippoli, plusieurs SCAF (systèmes de combat aérien du futur), composés chacun d'un nouvel avion de chasse et de drones qui étendront leurs capacités, formeront ensemble le système d'armes de nouvelle génération. Ce dernier, qui participera notamment à la guerre électronique et au recueil de renseignement, sera entièrement interopérable avec les forces aériennes alliées. L'IA sera utilisée dans le SCAF notamment pour : la reconnaissance d'images et vidéos (moyens optique, infrarouge et radar) traitées à bord ; le traitement et la génération de langage naturel pour l'interface homme-machine ; la reconnaissance de formes et la fusion de données pour la maintenance prédictive, le dépannage, la connaissance de la situation, la cybersécurité et l'hypervision ; l'autonomie pour la coordination d'essaims de drones et les systèmes collaboratifs ; l'aide à la décision pour la gestion de la flotte et la planification de mission. Sur le plan tactique, le « cloud de combat multi-domaines » permettra la mise en réseau des forces aériennes, terrestres, maritimes, cyber et spatiales. Il permettra d'exécuter, mieux et plus rapidement que l'adversaire, la boucle OODA : Observation, par la gestion et la fusion des capteurs de renseignements d'origines image, électromagnétique et humaine ; Orientation, pour la planification des missions ; Décision, pour le commandement et le contrôle ; Action, par le combat collaboratif.

Ecosystème. Les principaux algorithmes sont réalisés par les grands laboratoires et non par les startups, souligne l'ingénieur général Lemaire. Les grands groupes reviennent à la recherche fondamentale. Outre l'intégration de l'IA dans les systèmes futurs, il faut d'abord en mettre dans les systèmes existants pour augmenter leur performance à moindre coût. La souveraineté numérique varie selon les pays de l'Union européenne ou de l'OTAN. Une feuille de route nationale s'impose car les avis des Alliés évoluent.

Loïc Salmon

Allant de pair avec la mondialisation, la révolution numérique offre une façon de penser autrement le fonctionnement des Etats, des entreprises et des sociétés,

estime Julien Nocetti. La maîtrise des technologies de l'IA constitue un facteur de puissance en politique internationale. L'IA repose sur la collecte de masses considérables de données, collectées par les géants américains du numérique (Google, Apple, Facebook, Amazon et Microsoft) et chinois (Baidu, Alibaba, Tencent et Xiami). L'écosystème de l'innovation devient très compétitif. Sur les 4.500 entreprises traitant de l'IA, la moitié se trouve aux Etats-Unis et le tiers en Chine. Depuis 2013, Chine, Russie et Inde relocalisent des données sur le plan national. La Chine va investir 150 Mds\$ dans l'IA jusqu'en 2030. Dans 10-15 ans une rivalité entre la Chine et la Russie dans ce domaine pourrait s'ajouter à celle en cours entre les Etats-Unis et la Chine. (voir sur la photo la déclaration du président russe Vladimir Poutine).

Défense : l'IA, facteur décisif de supériorité opérationnelle

Défense : l'emploi de l'IA sur le champ de bataille de demain

Chine : l'intelligence artificielle, priorité de sécurité nationale