BRENNUS 4.0

LETTRE D'INFORMATION DU CENTRE DE DOCTRINE ET D'ENSEIGNEMENT DU COMMANDEMENT

Mars 2020

Systèmes d'information, intelligence artificielle et cybersécurité

Par Mesdames Claire Angelotti et Clarisse Naegels, rédactrices du pôle études et prospective du CDEC

Depuis les années 2000, les différents textes officiels relatifs à la défense et la sécurité nationales - Livre blanc, Revue stratégique, loi de programmation militaire - mettent l'accent sur la « connaissance et l'anticipation » en tant que fonction stratégique des Armées. Pour assurer cette fonction stratégique, et dans le but de garantir une supériorité opérationnelle des forces françaises, la maîtrise de l'information et l'optimisation des systèmes d'information de défense sont devenues des enjeux majeurs pour les Armées. Le développement de l'intelligence artificielle (IA) modifie aujourd'hui l'utilisation des systèmes d'information et le traitement des données. Souvent décriée comme une vulnérabilité cyber, l'IA est aussi une opportunité dans le domaine de la cyber-sécurité.

Les systèmes d'information

L'informatisation des tâches manuelles et la numérisation des Armées ont donné lieu à la création de multiples systèmes d'information utilisés à la fois pour le commandement, le renseignement, la préparation opérationnelle et la conduite des opérations. Dans un rapport de 2011, la Cour des Comptes définit les systèmes d'information et de communication (SIC) comme des « ensembles organisés d'acteurs, de procédures et de technologies permettant de saisir, de regrouper, de stocker, de manipuler, de protéger et de diffuser de l'information utilisée dans un ou plusieurs processus opérationnels ». L'objectif des systèmes d'information est donc de donner accès à l'information à tout moment et en tous lieux, d'en faire un usage opérationnel, de transmettre les ordres et d'assurer le partage de l'information (à un niveau interarmes, interarmées et interalliés). La numérisation des opérations est devenue un impératif stratégique et a favorisé le développement de flux d'information au sein de systèmes d'informations divers et variés. Au niveau interarmées, le programme SIA (Système d'Information des Armées) a été lancé en 2010 pour assurer une transformation des systèmes d'information

opérationnels et de commandement (SIOC) des trois armées et leur convergence en un seul et même système. L'objectif du programme est d'apporter une réponse opérationnelle aux besoins des Armées tout en s'inspirant des avancées provenant du monde civil. La multiplication des systèmes d'information

(SICF pour l'armée de Terre, SIC21 pour la Marine et SCCOA pour l'armée de l'Air) a constitué un défi pour l'interopérabilité des systèmes.

Le programme Synergie du COntact Renforcée par la Polyvalence et l'InfovalorisatiON (SCORPION), de l'armée de Terre va au-delà d'un renouvellement capacitaire et vise à développer le combat collaboratif grâce à l'évolution des systèmes d'information et de communication. Au niveau tactique, le système d'information et du combat SCORPION (SICS) doit pouvoir remplacer l'ensemble des SI déployés pour centraliser les données et la communication, harmoniser les systèmes et les rendre plus faciles d'utilisation. Le système d'information et du combat SCORPION est pensé comme un « système des systèmes » pour plus de cohérence. L'objectif est d'assurer un partage de l'information tactique et de favoriser l'interopérabilité entre les systèmes. SICS sera le système unique de référence pour le GTIA déployé. Ainsi se met en place une interconnectivité entre le GTIA, l'électronique des véhicules (vétroniques) et les systèmes de communication radio CONTACT.

L'apport de l'IA dans les systèmes d'information

Qualifiée de « priorité de la défense nationale » par la ministre des Armées Florence Parly, dans son discours sur l'IA du 5 avril 2019, et comme « enjeu de puissance militaire » par la revue stratégique de 2017 et la LMP 2019-2025, l'IA est au cœur de la stratégie de transformation du ministère. Révolution pour l'armement digitalisé, mais surtout pour le traitement des données et de l'information, elle requiert toute l'attention des armées. Les systèmes d'information ont favorisé le développement de flux massifs de données qui ne peuvent pas être traités par l'être humain. Il n'existe pas de définition commune de l'IA et la notion même d'« intelligence artificielle » est débattue. Néanmoins, le rapport de la Task Force IA, publié en septembre 2019, se réfère à la définition du Journal Officiel qui définit l'IA comme un « champ interdisciplinaire théorique et pratique qui a pour objet la compréhension de mécanismes de la cognition et de la réflexion, et leur imitation par un dispositif matériel et logiciel, à des fins d'assistance ou de substitution à des activités humaines ». Dans l'ensemble, l'IA consisterait donc à reproduire des moyens cognitifs par l'utilisation d'algorithmes. Il serait plus juste de parler d'automatisation ou d'« intelligence augmentée », puisque les apports de l'apprentissage automatique (*machine learning)*, en particulier l'apprentissage en profondeur *(deep learning),* montrent bien que les capacités de l'IA dépassent celles de l'être humain dans des domaines particuliers, tels que la reconnaissance d'objets sur des images ou vidéos.

Selon l'expression de Michael C. Horowitz, dans le domaine militaire, l'IA n'est pas une arme mais un facilitateur qui permet entre autres une meilleure gestion de l'environnement opérationnel et une meilleure préparation opérationnelle. Elle est une rupture dans le domaine de la détection des menaces et du traitement du renseignement, de la réception des données jusqu'à leur analyse et représentation (ou visualisation). L'IA se construit dans la continuité de la transformation numé-

rique et elle apporte une réponse aux défis du *big data*. Elle permet d'aller plus loin que le traitement automatique des données. L' apprentissage automatique et l' apprentissage en profondeur ont permis la réalisation de réseaux multicouches qui permettent d'analyser de façon plus rapide et précise les données. La machine apprend de ses erreurs et se perfectionne de trois façons, soit par renforcement, soit de façon supervisée, soit de façon autonome. Si la trajectoire de la future exploitation militaire de l'IA se dessine progressivement, il est certain que le politique jouera un rôle primordial dans la réalisation de cette dernière. Toutes les nations-cadres du développement de l'IA ont élaboré des plans d'action. Face à la Chine qui a lancé son programme en 2017 et qui souhaite obtenir le leadership en matière d'IA, la France pourrait s'inscrire dans des partenariats européens et civilo-militaires pour le développement d'une IA souveraine et indépendante.

La cyber-sécurité et l'IA

Deux logiques s'affrontent autour de la notion d'IA : la vision utopique d'un monde connecté et optimisé par l'IA s'oppose à une vision apocalyptique de l'IA, porte ouverte à tous les dan-

gers cyber. L'objectif n'est pas de lutter contre l'IA, mais de trouver un équilibre entre l'amélioration qu'elle apporte et les inconvénients qu'elle induit, pour pouvoir définir les règles d'encadrement à créer et faire de l'IA une alliée fiable, stable et précise. Il faut identifier les risques induit par l'IA, comme le vol de données massives, mais ne pas s'y arrêter. Les évolutions technologiques sont aussi bien utilisables par l'ennemi que par nos forces armées. En effet, les IA servent à la fois pour l'attaque (systèmes dotés d'IA capables de résister au système défensif et donc de détecter et contourner son utilisation à des fins sécuritaires) et la défense (systèmes dotés de l'IA pouvant repérer et traiter simultanément les virus).

La question de la place de l'homme dans la boucle se pose alors. Dans son discours sur l'IA, la ministre des Armées Florence Parly a insisté sur ce point, affirmant que « quel que soit la degré d'automatisation, voire d'autonomie de nos systèmes d'armes actuels et futurs, ceux-ci resteront subordonnés au commandement humain ». Parmi les vulnérabilités induites par l'IA, l'apprentissage automatique expose les armées et les industriels à des leurres, détournements ou attaques pendant la phase d'apprentissage, à l'instar de l'attaque dont a été victime le *chatbot TAY* de Microsoft. L'IA peut également être utilisée dans la guerre informationnelle. Couplée aux capacités biométriques, de reconnaissance faciale ou vocale, elle pourrait imiter la voix ou le comportement d'une personne, contribuant ainsi à la désinformation.

Toutefois, l'IA est aussi une opportunité pour lutter contre les menaces cyber. Elle peut en effet apporter une plus-value dans le domaine de la détection. Selon une étude de *The Independant IT-Security Institute*, 855 millions de virus ou logiciels malveillants auraient été créés en 2018. Ainsi, face à une création variée et constante de logiciels malveillants, les méthodes de protection cyber classiques semblent manquer d'efficacité. L'IA permettrait d'identifier et de détecter un virus beaucoup plus rapidement grâce à l'apprentissage automatique et à la détection de signaux faibles. Jusqu'alors, il était nécessaire de détecter le virus pour l'appréhender. Grâce à l'IA, la plupart des virus pourraient être détectés en amont puis traités. La société britannique *Dark Trace* a ainsi élaboré l'outil d'apprentissage automatique le plus avancé au monde. Inspiré du système immunitaire humain, ce système détecte et combat automatiquement le virus même si celui-ci n'a jamais été rencontré auparavant.

Enfin, l'IA assure une fonction de protection. L'homme est le maillon faible de la sécurité informatique ; l'utilisation accrue du *cloud* et des objets connectés (20 milliards d'ici 2020 selon une étude effectuée par l'agence *Gartner*) augmente les vulnérabilités du cyberespace. Ainsi, l'IA permettrait de renforcer la sécurité des systèmes d'authentification. Grâce à l'apprentissage en profondeur, l'IA serait en mesure d'enregistrer une empreinte digitale, une empreinte de la rétine ou encore de la paume de la main. Ajoutée au système classique d'authentification, l'utilisation de la biométrie améliorerait grandement l'intégrité de nos données et empêcherait, à terme, la pénétration d'un logiciel malveillant dans une entreprise, un opérateur d'importance vitale ou même dans un service de l'État. La *Defense Advanced Research Projects Agency* (DARPA) élabore ainsi un système d'authentification dite « active » ayant pour but de constituer une « signature cognitive » à partir de l'observation de l'attitude de l'usager lorsqu'il manipule l'outil informatique. En complément de la doctrine cyber défensive de la France, la ministre des Armées Florence Parly a annoncé en janvier dernier la mise en place d'un volet cyber offensif. Cette mesure démontre l'importance croissante du cyberespace et son aspect belliqueux. Enfin, la signature en novembre dernier d'une « convention cyber » entre le ministère des Armées et les représentants de 8 industriels stratégiques de la défense, illustre l'intégration progressive des enjeux de cybersécurité dès le développement des systèmes d'armes et des systèmes d'information.

Si l'IA peut être une solution pour faire face à l'augmentation des flux d'informations, favorisée par le développement des systèmes d'information, elle est aussi une opportunité pour lutter contre les risques cyber. Plus performante que l'humain dans le domaine de la détection, l'IA devrait pouvoir assurer une fonction de protection des réseaux. Au travers du programme SCORPION, l'armée de Terre souhaite intégrer cette technologie à ses systèmes d'armes. Compte tenu de son faible niveau de développement actuel, l'intégration de l'IA dans les systèmes d'armes prendra néanmoins du temps ; un temps probablement nécessaire à une meilleure adaptation du matériel et des forces à cette technologie.