Défense : l’essor du numérique sur le champ de bataille

La souveraineté numérique d’un Etat repose sur l’emploi des technologies civiles et militaires et sur le contrôle humain des systèmes d’information et d’aide au commandement.

L’Association des auditeurs de l’Institut des hautes études de défense nationale a organisé, le 4 octobre 2017 à Paris, un colloque sur ce sujet, auquel ont participé des experts et de hauts responsables dans les domaines du numérique et du renseignement.

Du possible à l’utile. Les « Big Data » civils fournissent des données nécessaires à la conception d’une opération militaire (renseignement, météo et cartographie). L’ensemble des données produites sur le champ de bataille doit être structuré et filtré explique un expert. Mais algorithmes, Big Data et intelligence artificielle (IA) ne peuvent prédire l’avenir ou déterminer une dangerosité. L’analyse géopolitique reste du ressort des chercheurs universitaires. Les services de renseignement essaient de comprendre un mouvement de société dans un pays donné et d’anticiper les réactions de ses dirigeants. Ils tentent aussi de recueillir l’information secrète et certaine, pour éclairer la décision de leurs propres autorités politiques et militaires. Ils aident aussi les forces de sécurité à neutraliser les menaces, par des renseignements précis, réels ou crédibles. L’IA automatise des recherches, impossibles à l’échelle humaine, pour déceler des

tendances. Par exemple, le contact entre un individu potentiellement djihadiste et son donneur d'ordre s'établit par le biais de plusieurs autres personnes. Or, les divers membres de cette filière lancent des milliers d'appels téléphoniques, dont seuls des algorithmes parviendront à trouver rapidement l'information pertinente. L'arrestation d'individus suspects permet de récupérer des données sur les modes opératoires (clandestinité, communication et action) et ainsi de détecter certaines similitudes. Enfin, les algorithmes réalisent des traductions automatiques des langues les plus pratiquées dans le monde, mais pas encore des plus rares.

Le pourquoi avant le comment. Depuis l'apparition d'internet en 1971 puis du GPS en 1991, les armées savent gérer les ruptures technologiques. Mais, estime un général, l'intelligence collective l'emporte souvent sur l'IA pour la réalité stratégique. Les regards convergents de tous permettent de conserver du discernement pour hiérarchiser les informations et leur donner du sens. La vigilance s'avère nécessaire sur les plans juridique (lois sur la sécurité et le renseignement) et pédagogique (définition de l'IA et de ses limites d'emploi). Outil de corrélation des données pour obtenir un résultat, l'IA dispose de la puissance de calcul pour trier les informations, nombreuses, incertaines, évolutives ou incomplètes (images, écoutes spécifiques et réseaux sociaux). La pléthore d'informations techniques entraîne le besoin de renseignements d'origine humaine pour mettre les conclusions en perspective. Le renseignement donne la capacité de conserver l'autonomie d'appréciation, d'organiser de la résilience et d'envisager le temps d'après la crise. Destiné à l'action et aux opérations, le renseignement technique nécessite de petits démonstrateurs, l'union des talents pour l'innovation et la création de synergies de proximité. En matière d'armement, poursuit le général, l'impact du numérique doit en être évalué dès sa conception. Ensuite, conformément à une doctrine d'emploi et un cadre juridique, les armées peuvent recruter des spécialistes et former des sous-officiers compétents pour les besoins opérationnels. Créativité et inventivité s'imposent face à l'adversaire, bien équipé lui aussi.

Réduire les incertitudes. Pour aider la décision opérationnelle en temps réel, le renseignement se doit d'être très réactif et collaboratif, explique un expert du numérique. Destiné à réduire les incertitudes, l'algorithme militaire intègre les paramètres de la mission, des règles d'engagement (ouverture du feu) et des contraintes légales et traite les données sur le contexte de la situation et la véracité des informations. Il s'inscrit dans la boucle OODA : Observer et Orienter

pour évaluer la situation, Décider et Agir pour la gérer. L'acquisition de renseignements, par la captation de données en environnements hostiles ou inconnus et la détection de signaux faibles par l'IA, va de pair avec l'automatisation de certains processus, en vue d'assurer une permanence. L'orientation inclut : l'analyse de la situation en temps réel ; l'interconnexion/analyse avec d'autres systèmes ; la consultation de bases de données tactiques ; la comparaison avec les modèles établis ; la construction d'une image mentale de la situation ; les propositions de choix possibles. Lors de la prise de décision, l'algorithme aide au choix, libère le stress du combattant ou du chef et contrôle le respect des règles d'engagement. L'action porte sur la précision, la délégation de tâches et le suivi de la cible. Les nouvelles technologies du numérique exercent déjà des effets sur le combat, poursuit l'expert. D'abord, les drones sont devenus indispensables au renseignement militaire. Les données sont enrichies, notamment par l'usage des jumelles multifonctions, dont la thermie. L'analyse des données s'externalise et/ou s'automatise. La réduction du cycle OODA permet de prendre l'initiative et de la sauvegarder. Il s'agit de trouver le renseignement très en amont, puis de riposter immédiatement et avec précision. Le combat dans l'espace numérique se caractérise par l'hyperconnexion et le traitement de l'information en temps réel en « local » (ordinateur de l'utilisateur) ou « déporté », grâce au « cloud » tactique. Le « cloud » héberge à distance de grandes quantités d'informations, accessibles de manière quasi instantanée. Au niveau tactique, il permet de recourir, en cas de besoin, à des données sur le théâtre d'opérations non stockées en local. Toute donnée présente un caractère critique pour les systèmes militaires, en qui les utilisateurs doivent d'abord avoir confiance. En outre, la surveillance des réseaux est devenue permanente pour la sécurité et la recherche du renseignement. « L'opération numérique » consiste à attaquer les systèmes d'information de l'adversaire, dont dépendent ses capacités militaires, pour le déstabiliser. Elle passe par la maîtrise préalable des systèmes hertziens et du cyberespace.

Loïc Salmon

Sécurité : l'intelligence artificielle, enjeu de souveraineté nationale

Armée de Terre : programme « Scorpion », le GTIA de demain

Renseignement militaire : clé de l'autonomie stratégique et de l'efficacité

opérationnelle

Les nouvelles technologies, potentiellement moins meurtrières, disposent d'une capacité de ciblage qui accroît l'effet de surprise, souligne un général. Mais elles effacent les frontières de l'espace géographique (drones militaires pilotés à partir du territoire américain), de l'espace militaire (dommages collatéraux des drones armés de la CIA, agence civile) et du contrôle à vue (furtivité des engins volants, invisibilité du cyber et discrétion des forces spéciales). La discrimination et la proportionnalité se diluent, faute de contact. La guerre entre dans un espace caché, hors des Etats et où tout est permis. En outre, face à l'automatisation, l'homme abandonne une part de responsabilité et son contrôle s'amenuise. Dans une guerre totalement dérégulée, la machine risque de l'emporter sur l'homme, avertit le général.