La cyberdéfense dans l'armée de Terre

Général d'armée Pierre SCHILL
Chef d'état-major
Armée de Terre

Il y a un « moment » pour l'armée de Terre

Les conflits qui font rage en Ukraine et au Proche-Orient transforment le fait guerrier dans des proportions et à une cadence inédites.

Terreau et réceptacles des innovations, ils bousculent la façon dont nous concevons et menons nos guerres. Un exemple, parmi tant d'autres : la transparence du champ de bataille - conséquence de l'emploi massif des drones et de l'accélération du cycle du renseignement - menace de rendre caduque le principe de concentration des efforts, théorisé par le maréchal Foch il y a plus d'un siècle. Surtout, la guerre cyber a bien lieu. Le département de cybersécurité ukrainien a annoncé avoir neutralisé 4500 cyberattaques russes en 2022 ; 1600 depuis le 1er janvier dernier. Le 7 octobre, le Hamas neutralisait le système d'alerte de la population israélienne Red Alert au moment où il franchissait la frontière israélienne.

L'armée de Terre a pris acte de ce tournant qui appelle l'adaptation des structures, du fonctionnement et de la doctrine.

La date du 24 février 2022 constitue une rupture, un changement d'ère stratégique. Elle met fin à un cycle amorcé il y a trente ans, né avec la première guerre du Golfe. Cette phase s'était traduite par une interarmisation accrue : création du Centre de planification et de conduite des opérations (CPCO), direction du renseignement militaire (DRM), création d'une école de guerre interarmées, intégration interarmées accrue dans les opérations extérieures. Le 24 février fait franchir aux armées une étape supplémentaire ; l'action simultanée sur terre, en mer et dans les airs ne suffit plus à remporter une bataille. L'efficacité opérationnelle et la légitimité de l'action passent par l'investissement de nouveaux espaces de conflictualité - cyber, cognitif et informationnel qui s'ajoutent aux précédents. Elles passent par la combinaison des effets dans tous les milieux (terre, air, mer, cyberespace et espace extra-atmosphérique) et champs (électromagnétique et influence).

La cyberattaque russe du 23 février 2022, la guerre des narratifs consécutive au bombardement de l'hôpital d'al-Shifa et, plus récemment, la médiatisation de la « madone de Marioupol » sont autant d'indices de cette interdépendance entre champs d'action - physiques - et nouveaux espaces de conflictualité - immatériels.

Un nouvel interarmées est ainsi né en 2022, résumé dans le concept militaire de « combat multi-milieux multi-champs », dit M2MC.

Sitôt qu'un espace s'offre à l'homme, il s'ouvre aux conflits

Pour l'heure, aucun « Pearl Harbor numérique » n'est à déplorer. Pourtant la composante cyber s'est imposée sur tous les théâtres d'opérations aux niveaux tactique et opératif.

Le conflit russo-ukrainien fournit notamment des mises en garde contre ce Janus numérique : si le téléphone épaule le soldat au même titre que son fusil - échange de renseignements, localisation ennemie, contre-influence en temps réel - il peut aussi le trahir en étendant sa surface de vulnérabilité - ciblage de soldats sur la base des ondes électromagnétiques émises.

Avant le conflit russo-ukrainien, le cyber était considéré comme un outil stratégique ; de fait, son rôle stratégique a été moins déterminant que l'explosion de son emploi tactique. Le théâtre ukrainien illustre l'intégration de la capacité cyber au sein des unités engagées au front. Il devient une composante d'appui indispensable pour protéger les unités et permettre la manœuvre.

Le cyber, un effort marqué de l'armée de Terre

L'ambition cyber de l'armée de Terre s'articule autour de deux impératifs : protéger l'autonomie de décision et accroître la capacité d'action.

L'armée de Terre n'a pas attendu le tournant de la guerre russo-ukrainienne pour investir le domaine cyber. En témoignent par exemple l'essor de la 807e compagnie de transmissions, unité de cyberdéfense, et la création d'un BTS cyberdéfense en 2020.

A ce jour, 50% du personnel militaire cyber des armées françaises sont ainsi rattachés à l'armée de Terre. Cette dernière porte son effort sur l'intégration de cette capacité dans la manœuvre de transformation interne qu'elle mène vers un nouveau modèle, dit armée de Terre de combat, selon une logique de déconcentration des moyens vers les unités.

Trois axes guident ce chantier.

- Actualisation de la doctrine : rapprochement des fonctions transmissions/SIC et cyber sous le parapluie « numérique » à travers un continuum SIC-SSI-LID, réaffirmation du commandement par l'intention afin de ne pas céder à la tentation de la centralisation de la prise de décision.

- Adaptation des structures : intégration de nos nouveaux commandements dans la boucle opérationnelle cyber - transformation du COM SIC en commandement de l'appui terrestre numérique et cyber ; création d'une unité spécifiquement dédiée à la contre-influence - la 712e compagnie de transmissions - et d'une seconde dédiée à la défense dans la profondeur de nos systèmes de commandement ; doublement des capacités du Centre interarmées des actions sur l'environnement (CIAE) de Lyon pour l'influence.

- Montée en puissance humaine et capacitaire : relever le triple défi du recrutement, de la formation et de la fidélisation ; acculturation des personnels actuels et embauche de spécialistes, doublement des compagnies cyber (de 2 à 4) ; actualisation des enseignements de l'école des transmissions, renforcement de la chaire cyber à Coëtquidan ; intégration de la LID à notre matériel - « LID embarquée ».

Pour l'armée de Terre, la cyberdéfense est un facteur de supériorité opérationnelle qui se superpose aux aspects les plus classiques de la guerre. L'enjeu est que ce domaine considéré jusqu'à présent de niveau stratégique devienne également un outil employé au niveau tactique jusqu'aux plus bas échelons.