Cyber : capacité interarmées, niveaux stratégique et tactique

Face au cyber, arme d'espionnage, de déstabilisation, de manipulation, d'entrave et de sabotage, la France organise une « chaîne cyberdéfensive » et emploie l'arme cyber dans les opérations militaires extérieures (Opex).

Florence Parly, ministre des Armées, l'a souligné le 18 janvier 2019 à Paris. A cet effet, 1,6 Md€ seront investis dans la lutte dans le cyberespace. En outre, d'ici à 2025, 1.000 « cyber combattants » supplémentaires seront recrutés au sein du Commandement de cyberdéfense (Comcyber), de la Direction générale de la sécurité extérieure et de la Direction générale de l'armement (DGA), dont les synergies et partages ont été renforcés.

Cyberdéfense de « bout en bout ». En 2017, le ministère des Armées a connu 700 événements de sécurité, dont 100 cyberattaques, nombre déjà atteint dès septembre 2018. En moyenne, plus de deux événements par jour ont touché le ministère, les opérations militaires, les expertises techniques et même un hôpital d'instruction des armées. Certaines attaques ont ciblé directement le ministère et d'autres ont visé des industriels et des pays partenaires de la France. Une nouvelle instruction ministérielle a été diffusée au sein du ministère pour que les

cadres, en situation de responsabilité, considèrent la maîtrise du risque cyber comme une priorité. En outre, un partenariat entre le Comcyber, la DGA et les grands industriels de défense, présenté lors du Forum international de la cybersécurité (Lille, 22-23 janvier 2018), permettra de protéger la communauté de défense.

Arme du champ de bataille. Plusieurs Etats incluent déjà les effets cyber dans leur stratégie militaire et leurs modes d'action et s'y préparent, à l'occasion d'exercices mettant en œuvre capacités conventionnelles et cyber. La ministre des Armées a rendu publics des documents sur les grands principes de la doctrine de lutte informatique offensive (LIO) à des fins militaires, tout en protégeant les éléments les plus sensibles pour garder la supériorité sur les théâtres d'opérations. La stratégie cyber des armées s'articule en quatre éléments. La DGA prendra en compte la doctrine dans la conception et le développement des armements futurs. Militaires et civils seront acculturés aux contraintes d'emploi de l'arme cyber. Le succès de la lutte informatique dépend de la coopération avec les pays membres de l'OTAN et de l'Union européenne. Enfin la compétence des combattants numériques lie expertise technique, finesse d'analyse et « savoir-être » militaire. Après l'intervention de Florence Parly, le général François Lecointre, chef d'Etat-major des armées auquel est rattaché le Comcyber, a présenté le spectre d'emploi, déjà en cours, des moyens de la LIO en Opex. Sur le plan stratégique, les effets portent sur : le renseignement à des fins de ciblage ou de développement capacitaire adverse ; la neutralisation d'un système de commandement stratégique ; la désorganisation des centres de propagande. Sur le plan tactique, la LIO amplifie les effets de l'action militaire, en complétant et renforçant l'arsenal offensif. Ses caractéristiques concourent directement à l'atteinte des grands types d'objectifs opérationnels. Le renseignement permet d'évaluer les capacités militaires adverses, grâce à l'extraction et au recueil d'informations. La perturbation ou la création de dommages majeurs facilite la réduction, voire la destruction, des capacités militaires et cyber adverses. La « déception » modifie les capacités d'analyse de l'adversaire et altère ses capacités de propagande. Enfin, la LIO s'applique dans le respect du droit international humanitaire.

Loïc Salmon

Cyber : nouvelle doctrine pour la lutte informatique

Cyberdéfense : soutien pour le renseignement, la protection, la prévention et l’action

Cyber : prise de conscience du risque et perspectives (2030)