Prise de parole du général d'armée François Lecointre

Séquence communication consacrée au « Cyber militaire »

MINARM - CEMA

Balard, 18 janvier 2019

Madame la Ministre,

Mesdames et messieurs,

- Mon propos s'inscrit en complément de ce qui vient d'être développé devant vous par la ministre des armées. Je traiterai plus particulièrement du cyber envisagé comme **arme d'emploi** dans nos opérations.
- La revue stratégique de défense et de sécurité nationale de 2017 et la revue stratégique de cyberdéfense de février 2018 ont reconnu le **rôle majeur** de la cyberdéfense militaire.
- Cette consécration a trouvé sa traduction dans la Loi de programmation militaire 2019-2025 qui a acté l'augmentation significative des **moyens** financiers et humains qui lui sont affectés.
- Cet effort vient répondre à une **nécessité** qui se fait chaque jour plus pressante.
- La compétition et la conflictualité ne se limitent plus, désormais, aux seuls milieux traditionnels, Terre, Mer, Air et à l'espace. Elles se sont étendues à ce **nouveau champ** au fur et à mesure que croissait l'utilisation des données numériques.
- L'originalité du cyberespace par rapport aux autres milieux est son origine **anthropique**. Ce milieu a en effet été entièrement façonné et créé par les hommes qui ont déployé des réseaux, les ont interconnectés et installé des serveurs pour que l'information soit traitée et distribuée.
- Cette singularité a plusieurs conséquences :
    - les contours et la structure de ce milieu ne cessent d'**évoluer** au gré des actions humaines, volontaires ou non.
    - C'est également un milieu d'une très grande **complexité** attachée à son caractère englobant avec des ramifications sur terre, dans l'air, en mer et dans l'espace.
    - Enfin, l'explosion de la numérisation soutient et favorise les métiers ; elle les organise. Le milieu cyber est un passage quasi obligé pour le développement d'activités.
- Il recèle par conséquent des potentialités de « désorganisation massive » qui ne doivent pas être ignorées mais au contraire intégrées dans une **pensée stratégique renouvelée**.
- C'est avec ce souci, qu'avec l'accord de la ministre des Armées, j'ai demandé au commandant de la cyberdéfense, le général Bonnet des Paillerets, de rédiger une **doctrine** de lutte informatique offensive (LIO) qui vous est présentée aujourd'hui au travers d'éléments de doctrine publics, la doctrine en elle-même étant secrète.

- Ces travaux doctrinaux témoignent de la volonté de **préparer l'avenir** des opérations militaires en intégrant graduellement cette nouvelle capacité à la manœuvre d'ensemble des armées.

***

[Une nouvelle stratégie pour une nouvelle conflictualité]

- Dans le domaine cyber – comme dans les autres champs –, la stratégie vise pour l'essentiel à acquérir et à conserver la supériorité (ou, tout au moins, une situation favorable) afin d'assurer la défense de nos intérêts et la préservation de notre souveraineté.

- La capacité à conduire des opérations militaires dans le cyberespace permet d'obtenir certains avantages sur les théâtres d'opération des armées.

- Comme l'a souligné la ministre des Armées, la lutte informatique défensive (LID) est essentielle à la protection de nos moyens dans la conduite des opérations mais il est possible d'aller au-delà. La lutte informatique offensive (LIO) peut être un formidable démultiplicateur d'effets.

- Celle-ci profite, en effet, de la mise en réseau croissante de l'ensemble des systèmes militaires et permet de tirer parti des vulnérabilités des systèmes numériques adverses.

- Elle élargit considérablement le champ des possibles et la palette des options modulables que je suis susceptible de proposer au Président de la République.

- Elle peut se combiner et, si nécessaire, se substituer aux autres capacités militaires de recueil et d'action sur tout le spectre des missions militaires résumé par le triptyque « renseigner – défendre – agir ».

- En réalité, les armes cyber apparaissent désormais comme des instruments incontournables de l'action militaire grâce à leur capacité à agir au profit des armes employées dans les autres milieux.

- Comme l'écrivait le stratège britannique John Füller bien avant l'existence du cyber : « *l'arme maîtresse n'est pas obligatoirement la plus puissante (…), ou celle qui assène le plus de coups : c'est l'arme qui ayant la plus longue portée, peut entrer la première en action et servir de couverture aux autres armes* ».

- Ce constat est transposable aux armes de LIO dont les potentialités ne cessent de s'élargir.

- Cela dit, elles ne sont pas pour autant la solution à tous les défis auxquels les militaires se trouvent confrontés sur les théâtres d'opération. La LIO ne rend pas obsolète l'action militaire traditionnelle. Elle en amplifie les effets en complétant et en renforçant l'arsenal offensif.

- Par ses caractéristiques propres, elle concourt très directement à l'atteinte de trois grands types d'objectifs opérationnels dans la conduite des opérations militaires :

    - **Renseignement** : extraction et recueil d'informations dans le but d'évaluer les capacités militaires adverses ;

    - **Neutralisation** : réduction voire destruction des capacités militaires et cyber adverses par la perturbation ou la création de dommages majeurs ;

    - **Déception** : modification des capacités d'analyse et altération des capacités de propagande de l'ennemi.

- Au plan stratégique, les effets de la LIO peuvent également être déterminants. Quelques exemples :
    - Renseignement à fins de **ciblage** ou de **développement capacitaire** ;
    - Neutralisation d'un système de **commandement** adverse de niveau stratégique ;
    - Désorganisation de centres de **propagande** adverses.
- C'est dans ce spectre d'emploi, que les armées ont engagé des moyens de LIO sur les théâtres d'opérations extérieurs, y compris au niveau tactique, sur lesquels elles sont présentes.
- Comme pour toutes les autres armes, l'emploi de l'arme cyber présente également des risques qu'il s'agit tout à la fois de circonscrire et d'assumer.

***

[La maîtrise des risques comme facteur de crédibilité]

- Les risques liés à l'emploi de la LIO découlent des caractéristiques propres au cyberespace qui est sans doute la manifestation la plus aboutie du double mouvement de dilatation de l'espace stratégique et de contraction corrélative du temps.
- Une fraction de seconde suffit pour que l'action numérique produise ses effets, aussi bien dans le champ virtuel que dans le champ physique.
- Immédiateté de l'action, dualité des cibles, hyper-connectivité sont autant de facteurs de risques qui ont été pris en compte dans l'élaboration de la doctrine ; tout comme la notion d'irrégularité.
- Les actions offensives auxquelles nous faisons face dans le cyberespace ont, en effet, souvent le caractère de l'**irrégularité**. Ce milieu favorise les actions de type guérilla ou de harcèlement. Trois raisons principales :
    - 1re raison : **la faible traçabilité** des attaques cyber qui sont très difficilement attribuables.
    - 2e raison : **la vulnérabilité**. La maîtrise du cyberespace est très difficile à conserver dans la durée compte tenu de l'étendue du milieu et de sa complexité.
    - 3e raison : **l'accessibilité aisée** pour les acteurs non-étatiques et les petits Etats. Un outil de LIO peut être aisément volé copié ou imité par des adversaires ou des acteurs tiers. Il possède rarement les contraintes associées à des armes du haut du spectre réservées aux Etats possédant une certaine maturité technologique.
- Ces caractéristiques nous imposent une maîtrise et un contrôle très stricts du choix des modes d'action et de l'utilisation des moyens en matière de LIO.
- Ce contrôle national de bout en bout vise notamment à éviter tout risque de détournement, de compromission ou de dommage collatéral d'une action dont les effets peuvent se propager au-delà de la cible visée en raison des interdépendances entre systèmes.
- La France est un Etat de droit attaché aux principes éthiques et au respect du droit international humanitaire. Elle n'envisage la LIO que dans le strict respect des principes de distinction, de nécessité, de proportionnalité et de précaution.

***

[La promotion d'un comportement responsable comme facteur de stabilité]

- La France cherche à promouvoir l'adoption de règles de comportement responsable et au développement de bonnes pratiques.

- Cette ambition se heurte assez naturellement à la logique complexe du cyberespace, à ses disparités d'organisation, de doctrines et de modes d'action.

- Néanmoins, ainsi que l'a souligné la ministre des Armées, la France et ses partenaires comprennent l'intérêt de promouvoir une culture de « cyber-responsabilité ».

- Notre pays joue et va continuer de jouer un rôle moteur dans la promotion d'une culture militaire cyber partagée entre partenaires européens, que ce soit au sein de l'OTAN ou de l'Union Européenne, notamment à travers l'IEI – Initiative Européenne d'Intervention.

***

[Conclusion]

- L'arme cyber est une arme d'emploi. Il n'est plus temps de tergiverser sur l'opportunité de s'en doter ou non.

- Elle doit être perçue comme un amplificateur des effets militaires traditionnels, autour d'une gouvernance robuste qui affirme le rôle du CEMA qui a autorité pour décider de son emploi dans le cadre des opérations militaires.

- Je remercie le COMCYBER pour le travail doctrinal qu'il a supervisé. Il va désormais avoir la tâche de coordonner les différentes actions qui en découlent. Je pense bien sûr à :
    - l'acculturation des militaires qui participent aux travaux de planification et de conduite des opérations,
    - la coordination de la mise en place des moyens offensifs au sein des forces, notamment par l'intégration de moyens au sein des unités combattantes ;
    - le développement de moyens de LIO dès la conception des équipements militaires.

- Il faudra pour cela relever le défi du recrutement et celui de l'innovation opérationnelle. Ce chantier est fondamental pour que soit confortée l'efficacité opérationnelle de nos armées.

- Je vous remercie.