MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Madame Florence Parly,

ministre des Armées

Présentation de la doctrine militaire

de lutte informatique d'influence

Paris, le 20 octobre 2021

– Seul le prononcé fait foi –

Madame la présidente, chère Françoise,
Mesdames et messieurs les parlementaires,
Monsieur le chef d'état-major des armées,
Mesdames et messieurs les officiers généraux,
Mesdames et messieurs les directeurs,
Mesdames et messieurs,

Nous avons tous, à portée de main, une fenêtre sur le monde.
Là, dans nos poches, nous avons tous, à portée de main, une fenêtre sur les rue de Kaboul, une autre sur certains villages du Sahel, sur ce qu'en dit la presse internationale et ce qu'en pensent les observateurs. Les observateurs, il s'agit de vous, de moi, de chaque personne qui se connecte à Twitter, Facebook, Instagram, Tik Tok ou Snapchat.

Aujourd'hui, 60 secondes, cela représente plus de 4 millions de requêtes *seulement* sur le moteur de recherche le plus utilisé au monde. 60 secondes, c'est aussi 4,7 millions de vidéos visionnées sur YouTube, des centaines de milliers de tweets, et 700 000 visites sur Instagram.

Et dans ce monde intégralement numérique, la révolution des réseaux sociaux, c'est aussi la révolution de l'information. Comme toute révolution, elle a emporté avec elle des espoirs et des progrès.
Elle a ouvert la voie à la libre circulation de l'information en temps réel, elle a donné une voix à celles et ceux qui n'en avaient pas, elle a élargi les horizons. Les réseaux sociaux ont permis de mobiliser des peuples entiers pour leurs libertés. C'est une caisse de résonnance qui a déjà prouvé l'étendue de ses pouvoirs.

Mais comme toute révolution, celle des réseaux sociaux engendre aussi des risques et de nouveaux dangers. Avec elle, nous avons vu grandir la propagation de *fake news*, la manipulation de certaines images, voire même des faits. Au cours de cette crise sanitaire, nous avons tous pu lire de fausses informations, aussi invraisemblables les unes que les autres, mais qui peuvent avoir un pouvoir dévastateur sur nos concitoyens.

Quand les réseaux sociaux amplifient les théories du complot et participent à répandre l'idée – absurde autant que mensongère – que le vaccin consiste à implanter des puces 5G pour surveiller la population, alors le constat est sans appel : **oui, la désinformation tue**.

Le fait est que les réseaux sociaux ont un pouvoir égalisateur : sur Twitter, la voix d'un utilisateur anonyme compte autant que celle d'un grand média dont la fonction essentielle est d'informer.

Aussi, la frontière entre les faits et les opinions se brouille. Les événements indiscutables et les commentaires autour de ces événements viennent à se confondre. Une opinion, quelle que soit sa provenance peut aujourd'hui avoir la même importance que les informations recoupées et vérifiées. Et nous voyons bien, quels sont les risques pour nos sociétés démocratiques lorsque des individus, mais aussi des organisations terroristes, voire des Etats utilisent ces moyens pour chercher à nuire ou à modifier notre perception de la réalité.

*

* *

Si nous sommes aujourd'hui devant vous avec le chef d'état-major des armées, c'est parce que nos opérations militaires n'échappent pas à la réalité des réseaux sociaux ; ou plutôt, parce que ce qui se passe sur les réseaux sociaux produit des effets réels sur nos opérations militaires.

Nos armées affrontent pleinement les conséquences des « opérations » qui sont conduites sur les réseaux sociaux : je pense par exemple aux campagnes qui sont conduites par des organisations terroristes, que ce soit pour recruter des combattants ou pour accroître leur influence.

Nos armées affrontent aussi les opérations destinées à saper la légitimité de leur action, notamment par la manipulation de l'information. Alors, je ne parle pas ici, bien sûr, des opinions qui peuvent être exprimées par des individus, je parle bien des opérations savamment élaborées et conduites par des organisations mal intentionnées, dans le but de nuire à nos armées.

L'information fausse, manipulée ou subvertie, c'est une arme. C'est une arme qui a permis à certains groupes terroristes de prospérer, et c'est une arme utilisée avec de plus en plus de résultats par nos compétiteurs stratégiques. C'est notamment ce que nous a montré le travail de l'actualisation de la Revue stratégique en 2020. **Le champ informationnel, c'est-à-dire l'ensemble des zones immatérielles de diffusion de l'information, est un lieu de compétition stratégique**.

*

Utiliser des informations fausses pour obtenir un avantage stratégique sur son adversaire, cela n'a évidemment rien de nouveau dans l'histoire des conflits. Le débarquement des forces alliées en Normandie en 1944 a été rendu possible par des opérations qui visaient à leurrer l'adversaire. Il existait même un comité secret de désinformation à Londres qui était spécifiquement chargé de diffuser de faux messages, notamment sur Radio Londres, pour laisser l'ennemi croire que le débarquement aurait lieu dans le Pas-de-Calais.

Et dès les années 1960, en pleine Guerre froide, les forces armées américaines et soviétiques intègrent ouvertement les opérations informationnelles dans leurs doctrines militaires. La faculté à agir sur la perception des populations était identifiée comme essentielle pour gagner la bataille idéologique. Alors, utiliser l'information comme une arme, comme je vous le disais : à l'ouest, rien de nouveau. A l'est, non plus, d'ailleurs.

*

Ce qui est nouveau, en réalité, c'est la vitesse à laquelle l'information circule dans le monde entier et c'est sa capacité à devenir virale. Et en cela, la révolution numérique a fait de l'information une arme, qu'on pourrait qualifier d'« hypersonique ».

La spectaculaire montée en puissance de Daech dans les années 2010 est pour beaucoup le résultat de sa capacité à mobiliser et à recruter sur les réseaux sociaux. Nous nous souvenons tous de ces vidéos effroyables d'exécution qui étaient diffusées sur Twitter. Daech s'est révélé être aussi une machine de communication terroriste extrêmement efficace. Son expansion territoriale est allée de pair avec la professionnalisation de ses opérations informationnelles. Et la neutralisation des cadres qui pensaient et qui orchestraient ces opérations a contribué au déclin de l'organisation et à la fin de sa domination territoriale. Nos efforts, couplés à ceux de nos alliés pour veiller l'espace informationnel, pour signaler des comptes suspects puis pour les faire fermer ont également réduit la visibilité de Daech. Cela a été l'un des succès de la Coalition internationale contre Daech, au même titre, finalement, que la victoire contre le pseudo-califat à Baghouz en mars 2019.

Lorsqu'elle est utilisée à bon escient, l'arme de l'information permet de gagner sans combattre. L'annexion de la Crimée par la Russie en 2014 est au moins autant le résultat des opérations informationnelles, de manipulation et de désinformation, que de véritables manœuvres militaires. L'éradication de débat en ligne au moyen de programmes automatisés (*bots*), la désinformation ciblée sur le Donbass ou encore les SMS annonçant volontairement à tort la mort de militaires ukrainiens à leurs familles ont fortement contribué à cette « opération éclair » de deux mois seulement.

Aujourd'hui, les principales puissances mondiales ne sont donc plus seulement engagées dans une course aux armements mais aussi dans une course aux technologies de l'information.

Nous devons aussi être conscients de l'asymétrie qui existe entre les démocraties libérales et les Etats autoritaires. Les citoyens ultra-connectés, qui partagent des informations et leurs avis en ligne peuvent, à leur insu, être transformés en acteur des conflits et en véritable proxy de l'adversaire. Ce risque, naturellement, n'existe que dans les pays où internet est un espace de libertés et non une zone de contrôle et de censure.

*

* *

Alors, parce que le champ informationnel est aujourd'hui un espace de conflits à part entière, j'ai pris la décision de doter nos armées d'une doctrine de lutte informatique d'influence.

La lutte informatique d'influence, cela désigne l'ensemble des opérations militaires conduites en appui de nos forces, dans le champ informationnel, pour détecter, caractériser, contrer des attaques ou appuyer la communication stratégique associée à une opération.

La supériorité opérationnelle est aussi informationnelle. Et sans nier nos valeurs, sans dévoyer les principes éthiques qui guident l'action de nos armées, nous devons être capables de faire face aux menaces qui existent dans le champ informationnel.

Nous ne pouvons pas prétendre protéger efficacement les Français si nous ne sommes pas capables de lutter contre ces menaces. Quand des appels à commettre des actes terroristes contre la France sont émis depuis le Levant, nos armées doivent être capables de réagir aussi vite que possible. La protection des Français en dépend.

Sur les théâtres d'opération où nos armées agissent, elles doivent donc pouvoir lutter contre la désinformation et contre la manipulation de l'information. Cela signifie être en capacité de limiter la propagation délibérée de fausses informations et d'informations biaisées à des fins hostiles.

Ce sont des opérations de cyberdéfense. Et en cela, la doctrine de lutte informatique d'influence vient compléter notre doctrine d'action dans le cyberespace qui comprend aussi la lutte informatique défensive et offensive, toujours en appui de nos opérations.

*

* *

Concrètement, cela signifie que sur les théâtres d'opération où elles agissent, les armées françaises conduisent des actions informationnelles afin de lutter contre la propagande terroriste et contre la manipulation de l'information.

Et si nous formalisons aujourd'hui l'objectif de lutte contre la propagande terroriste, il s'agit déjà d'une réalité opérationnelle pour nos armées. En lien avec le ministère de l'Intérieur, nos armées surveillent de près les activités numériques de Daech et d'Al-Qaïda depuis le milieu des années 2010.

En 2014, environ 46 000 comptes liés à Daech étaient recensés. En liaison avec nos principaux alliés, nos armées se sont employées à veiller les réseaux et à saisir toute occasion de contrer l'action numérique terroriste, en exploitant les renseignements recueillis et en dénonçant les comptes liés à cette propagande. La propagande de Daech a été nettement affaiblie par la combinaison de nos actions, ainsi que de celles de nos alliés, mais je voudrais aussi mentionner les efforts qui ont été faits pour que les opérateurs de réseaux sociaux prennent conscience de leurs responsabilités et, eux aussi, les assument.

Lorsqu'un post délibérément mensonger évoque sur un réseau social la neutralisation au Mali de 200 terroristes par des mercenaires, mercenaires dont la presse parle beaucoup ces temps-ci, nous ne pouvons pas ne pas réagir.

C'est un sujet hautement sensible et le terme d'« influence » pourrait laisser place à des interprétations maladroites ou mal intentionnées, c'est pourquoi je veux insister sur ce que la lutte informatique d'influence n'est pas, et sur ce que nos armées ne font pas et ne feront pas.

Ainsi, les armées françaises ne conduiront pas d'opération informationnelle sur le territoire national. Les armées françaises ne déstabiliseront pas un Etat étranger à travers des actions informationnelles qui viseraient, par exemple, ses processus électoraux.

*

Nous mettrons en œuvre ces opérations en veillant à ce qu'elles soient en parfait accord avec nos principes et nos valeurs. Comme l'ensemble des opérations qui sont menées par les armées françaises, la lutte informatique d'influence s'inscrit dans le strict respect du droit national et international, notamment la charte des Nations unies ainsi que les règles du droit international humanitaire. Cette nouvelle doctrine est d'ailleurs en parfaite cohérence avec les principes que nous avions mentionnés dans le Rapport sur l'application du droit international aux opérations dans le cyberespace, publié à l'automne 2019.

Dans le champ de l'information, être une démocratie pourrait, aux yeux de certains, être considéré comme une vulnérabilité. Comme je vous l'expliquais, les utilisateurs des réseaux sociaux en démocratie sont davantage susceptibles d'être instrumentalisés par nos adversaires.

L'asymétrie dans les conflits actuels est aussi une asymétrie éthique. **Garantir l'exercice des libertés individuelles, ce n'est pas une vulnérabilité. C'est une fierté. C'est une fierté de défendre les Français sans jamais renoncer aux valeurs qui font la France**.

Nous savons néanmoins que nous devons redoubler d'efforts pour renforcer nos moyens de défense, sans jamais renoncer à nos lignes rouges.

*

La loi de programmation militaire 2019-2025 avait d'emblée érigé la cyberdéfense en priorité, qui comprend donc la lutte informatique offensive, défensive ainsi que la lutte informatique d'influence. Les orientations qui ont été prises cette année suite à l'actualisation stratégique la LPM actuelle ont confirmé cette priorité et ont même amplifié la montée en puissance des équipements et des ressources humaines qui sont dédiés à la lutte informatique d'influence.

Pour conduire ces opérations informationnelles, les armées disposent déjà d'unités dédiées, placées sous le commandement du Comcyber. Déjà expérimentées en matière de lutte contre la propagande terroriste sur nos théâtres d'opération, elles élargissent leur spectre de compétence pour pouvoir lutter contre les manipulations de l'information sur ces théâtres, en se dotant d'outils de veille, qui sont inspirés notamment du modèle des unités américaines dites « Webops », qui appuient l'action des commandements stratégiques liés à chaque région du monde.

Je voudrais insister sur l'importance des ressources humaines employées à ce nouveau type de lutte, et je voudrais vous dire un mot des profils que nous recrutons pour nous défendre dans ce champ informationnel.

Nos cyberdéfenseurs de la lutte informatique d'influence - qui sont militaires ou civils de la défense - possèdent, au-delà d'une grande agilité sur les réseaux sociaux, des formations en sciences humaines qui leur permettent d'appréhender la sphère informationnelle particulière dans laquelle ils évoluent.

Certains parlent des langues rares, d'autres sont spécialisés en psychologie ou en technique numérique. Et tous exercent un métier passionnant et pour lequel des places seront à prendre dans les prochaines années.

Enfin, je voudrais souligner que nos unités de lutte informatique d'influence évoluent aussi dans un environnement dans lequel d'autres acteurs contribuent de façon déterminante au succès.

Je pense en premier lieu à nos alliés, dont plusieurs possèdent des capacités similaires que nous pouvons mettre à profit lors d'opérations en coalition. Je pense à certains acteurs privés, dûment sélectionnés, avec lesquels nous construisons les outils de veille qui sont les plus adaptés. Je pense aussi aux autres ministères, et en particulier au Ministère de l'intérieur qui, avec la plateforme Pharos, permet de signaler rapidement des contenus terroristes aux opérateurs de réseaux sociaux et très souvent d'en obtenir la fermeture. Et puis je pense enfin au ministère de l'Europe et des Affaires étrangères.

*

* *

Mesdames et messieurs,

Le Président de la République m'a donné un mandat clair : protéger les Français. Les protéger des menaces et des attaques, des conflits qui guettent et des capacités qui se créent.

Aujourd'hui, nous franchissons une nouvelle étape déterminante pour la défense des Français. Nous assumons, en appui de nos opérations militaires et dans le respect du droit, nous assumons d'agir dans le champ informationnel plutôt que d'en subir les attaques.

Aujourd'hui, nos armées se dotent donc d'un cadre clair pour s'armer et faire face aux menaces de la guerre par l'information. Car nous savons que nous avons tous, à portée de main, une arme que nos adversaires n'hésitent plus à employer.

Je vous remercie de votre attention et je cède maintenant la parole au chef d'état-major des armées.