Déclaration de Mme Florence Parly, ministre des armées, sur le volet de la cyberdéfense des armées, à Paris le 18 janvier 2019. (extraits)

=> en quoi ce discours constitue-t-il une inflexion de la politique française de défense ?

Depuis quelques années, le cyberespace est devenu un lieu de confrontation comme les autres. Un lieu où des milliers de hackers avancent masqués. Un lieu d'impunité où certaines nations se cachent pour mieux attaquer. Un lieu d'une immense violence, qui peut durablement nous bloquer (….)

Tout est possible dans le cyberespace. Se pensant protégés par l'anonymat de leurs claviers, certaines personnes, certains groupes et certains États, se croient tout permis. Leurs codes, leurs « bombes logiques » et autres *malwares* ont des effets bien réels. Tous les coups sont permis et peuvent avoir des effets. Ce phénomène est mondial ; il empire. Vous pouvez constater combien se multiplient les attaques venues de toutes parts, dont certaines résultent de stratégies de puissances. Et nous n'avons probablement encore rien vu. (….)

Le cyber est une arme d'espionnage, bien sûr, mais elle est aussi une arme que des États utilisent pour déstabiliser, manipuler, entraver, saboter. Et ce qui est vrai en temps de paix, le sera sans doute encore davantage en temps de crise, et en temps de guerre. Nous savons aujourd'hui, par exemple, qu'un certain nombre de nations incluent des effets cyber dans leurs stratégies militaires et leurs modes d'action, et s'y préparent à l'occasion d'exercices mêlant capacités conventionnelles et cyber.(….)

En 2017, le commandement de cyberdéfense a été créé. Il a prouvé sa pertinence et montré sa qualité. J'ai décidé d'en augmenter les moyens et d'en consolider la structure. La loi de programmation militaire prend acte de la menace cyber, c'en est même une priorité. Alors, nous renforçons nos effectifs et d'ici 2025, nous compterons au sein du COMCYBER, de la DGSE et de la DGA, 1000 cyber combattants supplémentaires. Nous renforçons les moyens avec 1,6 milliard d'euros investis pour la lutte dans le cyberespace.

En parfaite coordination avec l'ANSSI, l'autorité nationale de défense et de sécurité des systèmes d'information dont je salue l'expertise et la volonté, le ministère des Armées prend ses responsabilités pour la cybersécurité. Mais ma conviction, c'est que cet effort n'a de sens que s'il est collectif. Nous devons renforcer, ensemble, notre posture permanente de cyberdéfense, La cyberdéfense n'est pas une affaire de spécialiste mais bien de la responsabilité de tous. La maîtrise du risque cyber doit désormais être une priorité pour les cadres en situation de responsabilité. C'est bien l'esprit et l'objet d'une nouvelle instruction ministérielle qui vient d'être diffusée au sein du ministère des armées.(…)

Il nous faut anticiper, prévenir les attaques. Si elles surviennent, il nous faut les détecter, en réparer les effets, les caractériser et remonter si possible jusqu'à la source. Il nous faudra aussi répondre, j'y reviendrai.

Alors, pour réussir, nous devons nous coordonner encore plus. C'est un partenariat fort entre nos différents services, directions et armées qui permettra d'agir plus vite et plus assurément. C'est cette chaîne défensive unifiée, seulement, qui nous donnera de la cohérence dans nos actions et donc de la crédibilité et de l'efficacité.

Nous devons aussi nous tourner vers nos partenaires et nos alliés. Il n'y a pas de cyberdéfense sans alliance, pas d'alliance sans partenaire de confiance. Toutes les attaques ont une ampleur internationale.

Je pense à l'OTAN, qui permet coopérations et exercices pour notre cybersécurité. Je pense à l'Europe, aussi. Les menaces cyber pèsent sur tous les pays de notre continent et nous avons tout intérêt à unir nos efforts plutôt qu'à combattre en ordre dispersé. L'union fait la cyberdéfense et je n'imagine pas l'Europe de la défense sans son volet cyber. L'initiative européenne d'intervention, voulue par le Président de la République et lancée l'année dernière offre un cadre parfait pour des
partenariats cyber ambitieux et des réponses mieux coordonnées. (…)

En cas d'attaque cyber contre nos forces, nous nous réservons le droit de riposter, dans le respect du droit, par les moyens et au moment de notre choix. Nous nous réservons aussi, quel que soit l'assaillant, le droit de neutraliser les effets et les moyens numériques employés. (….)

Aujourd'hui, la France choisit de se doter pleinement de l'arme cyber pour ses opérations militaires. Nous considérons l'arme cyber comme une arme opérationnelle à part entière. C'est un choix nécessaire, en responsabilité. Nous en ferons un usage proportionné, mais que ceux qui sont tentés de s'attaquer à nos forces armées le sachent : nous n'aurons pas peur de l'utiliser.

Sur le plan opérationnel, le cyber est une capacité interarmées, sous l'autorité du chef d'état-major des Armées. Il s'agit d'une capacité de niveau stratégique, dans la conception et la manœuvre globale. Il s'agit aussi d'une arme au niveau tactique, dont les effets se combinent déjà sur le terrain à ceux des armes plus traditionnelles.Pour nous donner tous les moyens d'agir, avec à l'esprit le volet offensif de notre stratégie cyber, je vois quatre défis qu'il nous faut relever.

Le premier, c'est celui de la DGA. Il lui revient de prendre en compte cette nouvelle
doctrine offensive pour concevoir et développer les armements de demain.

Le deuxième, c'est celui de l'acculturation de nos militaires et de nos personnels civils à une arme aux contraintes d'emploi, à la fois nouvelles et spécifiques.

Le troisième défi, c'est celui de la coopération avec nos partenaires internationaux,
notamment européens.

Et enfin le dernier défi, c'est celui des compétences, le défi des ressources humaines.