MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Madame Florence Parly,

ministre des Armées

Paris Cyber Week

Paris, le 8 juin 2021

– Seul le prononcé fait foi –

Mesdames et messieurs,
Bonjour à tous,

C'est vraiment un grand plaisir d'être aujourd'hui avec vous pour clore cette première journée de la Paris Cyber Week. J'aurais assisté avec beaucoup d'intérêt aux tables rondes, dont les sujets sont tous aussi passionnants les uns que les autres et incontournables pour le ministère des Armées – de la désinformation à l'internet des objets, sans oublier évidemment la souveraineté technologique.

Cette souveraineté, elle ne s'arrête pas à nos frontières françaises, car justement, le cyber ne connait pas de frontière. C'est une souveraineté que nous devons concevoir dans un cadre européen. J'y reviendrai et j'imagine que les diverses tables rondes organisées sur ces deux journées ont abordé et aborderont ce sujet sous toutes ses facettes. C'est d'ailleurs un signal très fort de voir autant de nationalités rassemblées pendant deux jours pour discuter des enjeux cruciaux du cyber et plus largement du numérique.

Lorsque je parle d'enjeux cruciaux, je pèse mes mots. En tant que ministre des Armées, je ne peux que constater que le cyberespace est devenu un espace de conflictualité. Bien qu'il touche au champ de l'immatériel, il n'en demeure pas moins pernicieux et dangereux. Car il fournit des armes qui ont un potentiel d'obstruction, de destruction et de paralysie massives.

Nous en sommes ici tous conscients, l'espace numérique n'est pas un espace isolé du monde réel. Avec quelques serveurs et quelques ordinateurs, il est techniquement possible de provoquer la panne généralisée d'un groupe hospitalier. Cela s'est déjà vu. Ou de façon plus insidieuse, des logiciels espions peuvent infiltrer les systèmes d'entreprises ou d'institutions, et ce parfois pendant des années pour en extraire des informations. Alors évidemment, mon intention n'est pas de noircir le tableau ou d'avoir un discours anxiogène, au contraire ;

aux fantasmes je préfère la lucidité. **Et c'est donc avec lucidité que nous avons fait du cyber une des priorités au ministère des Armées.**

Aujourd'hui, notre supériorité opérationnelle, c'est-à-dire la capacité à garder l'avantage sur le terrain face aux acteurs malveillants, dépend de notre maîtrise du champ numérique. La résilience numérique doit donc aussi être repensée en intégrant fortement et à tous les niveaux, les enjeux de cybersécurité dans les organisations.

Pour notre ministère, cela signifie qu'il faut mieux anticiper les menaces, notamment à travers le renseignement et le développement de coopérations fortes. Il s'agit de détecter les attaques, de les caractériser et de se donner les moyens de les attribuer. Il s'agit de protéger de ces attaques nos réseaux dès leur conception, de les défendre mais aussi de pouvoir répliquer quand cela est nécessaire. Il s'agit enfin de permettre à nos forces qui sont en opérations de combiner les armes cyber avec les actions cinétiques, c'est-à-dire l'utilisation des armes conventionnelles, pour démultiplier les effets de nos interventions. Le cyber est une arme : la France s'en sert pour se défendre, mais s'il le faut, elle n'exclut pas de s'en servir de façon offensive lors de ses opérations.

A cet ambitieux programme de lutte dans l'espace numérique, nous consacrons 1,6 milliard d'euros d'investissements sur la période de la loi de programmation militaire 2019-2025 et nous intensifions comme beaucoup d'autres nos recrutements de sorte à disposer d'une armée de 4000 cyber combattants d'ici 2025, un effort de montée en puissance que j'ai décidé d'encore accélérer compte-tenu des enjeux.

Car le cyber n'est évidemment pas qu'une affaire de technique. C'est aussi une affaire de compétence, c'est donc une affaire humaine. **Aucun domaine technique ne s'est jamais conquis sans intelligence humaine.** C'est un enjeu qui concerne évidemment nos organisations,

nos compétences et nos talents. Car la cybersécurité est un domaine d'expertise qui requiert des compétences de très haut niveau.

Au cours de ces dernières années, le ministère des Armées s'est mis en ordre de bataille pour revoir la typologie des métiers, adapter les postes aux besoins nouveaux du ministère. Cette agilité est indispensable si nous voulons rester dans la course du numérique – plusieurs études[1] estiment en effet que 85% des emplois de 2030 n'existent tout simplement pas encore.

Aujourd'hui, les métiers de la cyberdéfense au ministère des Armées pourraient, de façon très schématique, être répartis selon quatre grands blocs : le bloc de la protection (comment résister face à une cyberattaque), le bloc du renseignement (comment collecter l'information utile dans l'espace cyber afin de l'analyser et l'exploiter), le bloc de la conception et du développement de systèmes complexes (comment concevoir les systèmes d'armes à l'aune des enjeux de cyberdéfense) et le dernier bloc, celui de l'action de combat (le combattant cyber, en particulier offensif).

Pour l'ensemble de ces grands blocs, nous recrutons des profils très variés, et contrairement aux idées reçues, ce ne sont pas tous des geeks en sweat à capuche et en tongs. Certes, nous avons besoin de développeurs qui portent des sweats à capuche et des tongs, capables de développer des solutions de cybersécurité, ou encore d'investigateurs numériques, ces sortes d'enquêteurs maniant avec dextérité le codage informatique et capables de fouiller les réseaux, logiciels ou autres supports numériques pour évaluer les dommages induits par un système compromis.

Mais nous avons aussi besoin d'un grand nombre de spécialistes en gestion de crise, de conseillers en planification et en conduite

[1] *Dell* et *Institute for the future*, 2017

d’opérations, ou de personnels sachant réaliser des audits de la sécurité de nos systèmes.

Je crois qu’il est essentiel de bien connaître et de faire connaître cette diversité des métiers et des possibilités dans le domaine de la cyberdéfense. Dans ce contexte, la formation est évidemment indispensable et nous avons aussi intensifié nos efforts en la matière. En septembre 2020, nous avons conclu un accord-cadre interministériel dans le domaine cyber qui associe 9 ministères et 54 établissements publics. Les masters et BTS spécialisés dans ce domaine se multiplient, aussi bien dans les grandes écoles de la défense des trois armées qu’en partenariat avec des écoles publiques.

Nous mettons naturellement l’accent sur les jeunes : depuis 2020, nous avons doublé le nombre d’apprentis en cyber. Nous multiplions les opportunités de sensibiliser nos futurs développeurs informatiques, nos experts en ciblage numérique, ou autres conseillers en opérations dans le cyberespace à nos métiers. En mars 2021, près de 400 étudiants se sont mobilisés pour entrer en immersion dans l’univers de la cyberdéfense et participer à DEFNET, cet exercice ministériel qui a pour objectif d’entrainer la chaine cyberdéfense au combat numérique.

Enfin, nous avons à cœur de faire participer l’ensemble des agents et personnels du ministère qui souhaitent travailler au profit de notre cyberdéfense. Nous accueillons un nombre déjà important de nouveaux cybercombattants et cybercombattantes civils comme militaires, sous contrat court ou sous statut de carrière, qui s’épanouissent pleinement dans les nouveaux métiers que nous leurs offrons.

Nous avons développé des formations et des passerelles à destination de celles et ceux qui ne disposent pas du tout de diplômes. **Dès que la motivation et l’envie sont là, il y a toujours une voie vers la cyberdéfense.**

Donc si je devais avoir un message aujourd'hui à destination de celles et ceux qui seraient tentés de rejoindre le domaine de la cybersécurité, et pourquoi pas au ministère des Armées, ce message est assez simple : venez tels que vous êtes. Il n'y a pas de parcours type, pas de cases à cocher. Notre objectif, c'est de grandir avec vous.

C'est un message que je veux répéter en particulier à destination des jeunes filles et des femmes. Nous avons besoin d'elles ! Le cyber a besoin des hommes, mais aussi des femmes qui représentent la moitié de l'humanité, de leur créativité et de leurs compétences. Je crois fermement que la révolution numérique est l'occasion de repenser profondément notre société et notre rapport au monde. Et nous ne devons pas être absentes de ce débat structurant pour l'avenir. Au contraire, il faut le porter avec force et saisir l'opportunité du numérique pour faire progresser nos sociétés vers plus d'égalité et plus d'inclusion.

Aujourd'hui au ministère des Armées, et je suis assez fière de le dire, 15% des postes cyber sont occupés par des femmes au ministère des Armées. C'est un chiffre en hausse, et je me réjouis de voir que chaque année, nous recrutons de plus en plus de femmes dans ce secteur : en 2020, 23% des personnes recrutées dans les métiers du cyber sont des femmes, contre seulement 13% en 2018, c'est-à-dire 10 points de plus en l'espace de 3 ans.

Ce résultat ne s'est pas obtenu par un coup de baguette magique, il tient beaucoup à l'action remarquable du réseau Combattantes@Numérique que je tiens à saluer. Depuis 2018, Combattantes@Numérique promeut la place des femmes dans les filières du numérique en fédérant des centaines de femmes issues de tous horizons, tous postes et tous âges. Ce réseau ministériel a vocation à s'ouvrir vers l'écosystème académique, industriel et européen. Je me réjouis notamment d'un partenariat en gestation avec Women4Cyber qui participe à cette Cyber Week et qui fédère les femmes présentes dans le secteur du numérique à l'échelle européenne.

Comme je vous le disais en introduction, le numérique est un domaine qui ne connaît pas de frontières : notre horizon, c'est l'Europe.

Une table ronde, me semble-t-il, sera consacrée demain à la présidence française de l'Union européenne. Le cyber figure évidemment parmi les priorités de notre présidence et nous comptons bien profiter de cette opportunité pour renforcer les liens entre les différents responsables nationaux et soutenir les projets européens qui sont dédiés à la cyberdéfense permanente. Nous devons en effet aller plus loin dans ce domaine, pour garantir l'accès des Européens à cet espace désormais contesté, et pour développer une culture mais aussi des outils efficaces de solidarité entre Européens. Car il ne faut pas se leurrer : si l'un d'entre nous est ciblé par une attaque, c'est potentiellement toute l'Europe qui peut être touchée. C'est un grand danger pour nos économies, pour notre sécurité, mais aussi pour nos démocraties. A cet égard, l'adoption en septembre 2020 par la Lituanie, la Lettonie et la France de la Déclaration sur la protection des démocraties a constitué un pas important vers une prise de conscience : celle de la nécessité de renforcer notre résilience face à ce type de menaces.

Dans le même esprit, le COMCYBER français participe à la conférence des *Computer Emergency Response Teams* militaires organisée par l'Agence européenne de défense. Nous fondons des espoirs importants sur ce cénacle pour bâtir la confiance mutuelle, améliorer les mécanismes de partage de l'information sur la menace cyber et identifier des possibilités de développement capacitaire à l'échelle européenne.

Nous devons donc nous entraîner ensemble, organiser des exercices au niveau européen pour, chaque fois que ce sera nécessaire, être en mesure de réagir ensemble. Nous devons par ailleurs renforcer nos capacités en la matière. Notre supériorité opérationnelle dépend étroitement de notre souveraineté technologique et par effet d'entrainement de notre souveraineté économique.

Nous devons avoir notre propre façon d'innover, en France et en Europe, car ce n'est qu'en développant notre industrie de défense nationale et européenne que nous aurons des entreprises fortes et capables d'innover au profit de nos armées et plus généralement de la société. Ainsi, investir dans notre économie de défense, c'est stimuler l'innovation technologique et c'est aussi renforcer de fait notre souveraineté militaire. Ce qu'on appelle dans le jargon de l'Union européenne la Coopération structurée permanente, un cadre de travail pour plusieurs Européens volontaires, pourra être un outil très utile pour renforcer nos capacités militaires de cyberdéfense. Et nous avons en particulier un projet coordonné par la Lituanie qui devrait être très prometteur.

Le Cyber est par ailleurs un domaine qui se prête particulièrement bien à la coopération entre l'UE et l'OTAN. La France a d'ailleurs été à l'origine avec le Royaume-Uni du *Cyberdefense pledge* de l'OTAN. Et le Centre d'excellence de Tallinn en Estonie a développé une expertise qui est reconnue au plan mondial.

J'aimerais aussi rappeler que nous avons déjà de nombreux projets de coopération avec nos partenaires européens. Nous partageons en temps réel les alertes, les informations et les menaces grâce à la connexion des Centres Opérationnels.

Au moment où sera lancée la présidence française de l'Union européenne en janvier 2022, le ministère des Armées tiendra la deuxième édition de La Fabrique défense, un événement unique tourné vers les jeunes Européens pour les sensibiliser aux enjeux de défense et pour faire émerger ce que l'on appelle une culture stratégique commune. Je suis très heureuse que la Paris Cyber Week soit le premier événement labellisé « La Fabrique défense », en avance de phase si je puis dire, c'est une belle reconnaissance de votre engagement européen et de l'importance du domaine cyber pour la défense européenne.

Alors, je vous donne rendez-vous l'année prochaine pour célébrer l'Europe et donner l'impulsion aux sujets technologiques qui seront au cœur de la présidence française de l'Union européenne.

Je vous souhaite des échanges très riches à venir, merci à tous.