Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DES ARMEES

Madame Florence Parly,

ministre des Armées

Inauguration du bâtiment « Commandant Roger Baudoin »
du Commandement de la Cyberdéfense du ministère des Armées

Rennes, le 3 octobre 2019

– Seul le prononcé fait foi –

Monsieur le préfet,
Mesdames et messieurs les élus,
Monsieur le directeur général de la sécurité extérieure,
Général, commandant la cyberdéfense,
Madame l'ingénieure générale directrice du centre DGA-MI,
Messieurs les officiers généraux,
Chers cyber combattants et combattantes, chers agents civils et militaires du Comcyber,
Mesdames et messieurs,

Un centre de commandement des opérations privé de moyens de communication. Notre industrie de défense à l'arrêt. Des sites gouvernementaux affichant des messages haineux en guise de page d'accueil. Des drones à la trajectoire manipulée et détournée. Tels pourraient être les méfaits de cyberattaques massives. Et dans l'obscurité de ce qu'elles pourraient engendrer, subsiste une lueur brillante et persistante ; celle de notre armée de cybercombattantes et de cybercombattants sur le pied de guerre, prête à détecter, attribuer, contrer ces attaques.

Alors, non, je n'ai pas l'intention de donner des idées aux scénaristes de *Black Mirror*, pas plus que je n'ai l'intention d'avoir un discours anxiogène sur les conséquences possibles d'une cyberattaque majeure. Au contraire, imaginer ces situations, anticiper les effets que pourraient avoir ce que les spécialistes appellent depuis quelques années un « Cyber Pearl-Harbor », c'est justement se mettre en ordre de bataille pour l'empêcher. Et le ministère des Armées est prêt. Nos armées, la Direction générale de l'armement, la DGSE et notre outil industriel de défense sont prêts à faire face à ces nouvelles menaces, à garantir notre souveraineté nationale, en lien étroit avec l'ensemble des autres acteurs concernés, au premier rang desquels je voudrais bien sûr citer l'ANSSI, l'agence nationale de la sécurité des systèmes d'information.

Nous avons dans le cadre de la Loi de Programmation Militaire, affirmé avec force nos ambitions dans le cyberespace. J'ai eu l'occasion de présenter notre stratégie de cyberdéfense il y a un peu moins d'un an, et nous avions alors pris de court beaucoup d'acteurs en rendant publique notre doctrine de lutte informatique offensive. Cette approche offensive complète évidemment toute une stratégie défensive d'anticipation, de prévention, et d'identification des menaces. Elle lui donne également cohérence et crédibilité.

La cyberdéfense, dans ses dimensions défensive et offensive, s'est donc imposée comme une capacité nouvelle, intégrée à part entière à nos opérations militaires. Mais elle suppose le développement de nouvelles compétences, elle demande à repenser la préparation opérationnelle de notre cyber-armée et pose aussi de nouvelles questions, notamment juridiques.

*

A la suite de l'Appel de Paris du 12 novembre 2018, et de la déclaration lancée par le Président de la République en faveur de l'élaboration de principes communs pour la sécurisation du cyberespace, j'ai souhaité que nous clarifiions l'application du droit international aux opérations dans ce nouvel espace, en temps de paix comme en temps de guerre.

J'ai donc chargé un collège d'experts juridiques du domaine cyber d'établir un rapport explorant les modalités d'application du droit international aux opérations dans le cyber espace, en temps de paix et en temps de conflit. Le commandement de la cyberdéfense et la direction des affaires juridiques, en lien avec la direction générale des relations internationales et de la stratégie ont été en première ligne de ces travaux, dont je tiens à souligner l'immense qualité.

Grâce à cet excellent rapport, rendu public le mois dernier à l'université d'été de la défense, la France dispose aujourd'hui d'un socle juridique de référence permettant de partager sa vision du droit des opérations dans le cyberespace ; et c'est une vision qui distingue le temps de paix et le temps de conflit armé.

A ce jour, nous sommes le seul et le premier pays à avoir pris position et ouvert la voie à l'application du droit international dans le cyberespace. Ce rapport est le premier à tenter de définir la notion de temps de paix et de temps de conflit dans l'espace numérique. Il est aussi la preuve de notre constant engagement en faveur du respect du droit international ; et le cyber n'y fait pas exception.

C'est un document fondateur et nécessaire au moment où les négociations portant sur les enjeux de cybersécurité reprennent à l'ONU. Il nous sera précieux pour partager notre vision pour un cyber espace de confiance et pour appuyer nos positions lorsque seront abordées les questions relatives à l'application du droit international dans le cyberspace. Et je tiens à réaffirmer ici un principe inaliénable qui nous guidera lors des discussions à l'ONU : nous conserverons toujours notre autonomie d'action dans le cyberespace.

Une des conditions pour la conserver et agir en toute indépendance, est d'assurer la résilience de nos systèmes. En janvier dernier, j'avais annoncé notre ambition de créer une chaîne cyberdéfensive « de bout en bout » qui protège autant nos forces que notre industrie et nos activités de maintenance. Je suis ravie de pouvoir vous dire que ce maillage sans faille de nos compétences cyber sera bientôt une réalité.

Le Commandement de la cyberdéfense et la Direction générale de l'armement, en collaboration avec l'ANSSI (Agence nationale de la sécurité des systèmes informatiques) ont en effet travaillé main dans la main avec huit grands maîtres d'œuvre industriels pour structurer et sécuriser de bout en bout la chaîne de production et de soutien des équipements militaires. Nous signerons prochainement une convention formalisant ce partenariat voué à rehausser le niveau de cybersécurité de nos systèmes existants et futurs : cet accord doit en effet faciliter et encourager la concertation autour de l'évolution des dispositifs de cyber et améliorer leur prise en compte dès la naissance des programmes d'armement. Cet accord illustre aussi la communauté de destin et d'ambition qui lie la cybersécurité de nos Armées à celle de notre industrie de défense.

*

Car vous le savez, la cyberdéfense est une priorité absolue du ministère des Armées. Nous investissons beaucoup, nous recrutons à un rythme soutenu, nous consolidons nos pôles d'expertise dans les armées, à la DGA et à la DGSE avec l'ambition de donner à la France les moyens de construire une cyberdéfense à la hauteur de ses ambitions opérationnelles et de faire de la France un acteur incontournable de la cybersécurité.

Et si je suis aujourd'hui à Rennes, c'est parce que c'est ici que se concrétise une grande partie des efforts qui est réalisée pour bâtir notre cyberdéfense. Je commencerai par un chiffre : d'ici 2025, nous aurons une armée de 4 000 cybercombattants, soit 1 000 de plus qu'aujourd'hui. Sur ce millier de recrutements, 800 seront opérés dans le bassin rennais.

Choisir Rennes était une évidence. C'est ici que nous avons développé dès 2014 un pôle d'excellence cyber en partenariat avec la région. C'est ici qu'est ancré le centre d'expertise de maîtrise de l'information de la DGA, référent en matière de cyber depuis plusieurs décennies. C'est enfin ici que le Comcyber a pris en partie ses quartiers.

C’est donc une véritable « cyber-vallée européenne », que nous construisons avec la Bretagne, qui a fait de la cybersécurité une des priorités de sa stratégie de développement économique, d'innovation et d'internationalisation.

Aujourd’hui, on dénombre près de 70 entreprises du secteur de la cybersécurité sur Rennes Métropole. Des PME aux laboratoires, des universités aux fonds de capital-risque ou encore de la région aux grands groupes industriels, tous les acteurs du territoire s’attachent à construire et perfectionner avec talent l’expertise française en matière de cyber.

Et je suis très heureuse d’inaugurer aujourd’hui, au cœur de cet environnement unique le premier bâtiment entièrement dédié à la conduite des opérations cyber. Ce bâtiment, nous avons choisi de le baptiser en hommage au commandant Roger Baudouin, l’un des premiers et des meilleurs cryptographes de l’armée française, celui qui a formé Alan Turing à la cryptologie. Ce même Alan Turing, qui déchiffra la machine Enigma, conférant ainsi aux Alliés un avantage considérable durant la Seconde Guerre mondiale. Je porte l’espoir que l’histoire du commandant Baudoin inspire nos cybercombattants et toutes les personnes qui entreront dans ce bâtiment, temple de la cyberdéfense, contenant, je vous le livre pour l’anecdote, plus de 200 kilomètres de câbles informatiques.

Et ce n’est que le début. Car ce bâtiment n’est que le premier. Conformément aux engagements de la loi de programmation militaire, deux nouveaux bâtiments permettront au Comcyber de disposer d’un outil redoutable de planification et de conduite des opérations dans le cyberspace. Ces moyens qui placent la France à l’avant-garde des opérations sont la traduction concrète de l’élan du ministère en matière de cyber. Ils illustrent aussi notre volonté de nourrir l’ambition cyber qui prévaut ici, à Rennes.

Cette dynamique permettra de renforcer les synergies entre les différents acteurs de la cyberdéfense du ministère, notamment entre le commandement de la cyberdéfense, la direction générale de l'armement et les équipes de la direction interarmées des réseaux d'infrastructures et des systèmes d'information. Rapprocher, voir réunir toutes les compétences stimulera nos capacités d'anticipation, de caractérisation et d'attribution des cyberattaques. Les infrastructures du quartier Stéphant permettront de mutualiser et d'optimiser la préparation opérationnelle de nos cyber combattants et combattantes sur l'ensemble du spectre de la lutte informatique.

Nous devrons également profiter de l'environnement académique du bassin rennais, riche de chercheurs et laboratoires, de l'Ecole des Transmissions, de l'Institut Mines Télécom ou bien encore de Centrale Supélec. Et nous pourrons compter sur le pôle d'excellence cyber développé en partenariat avec la région Bretagne qui a déjà tissé de nombreux liens avec le tissu universitaire environnant. Je rappelle également que les écoles de Saint-Cyr Coëtquidan et l'Ecole Navale ont chacune une chaire de cyberdéfense. C'est indéniablement dans le bassin rennais que se forment nos prochains cyber-combattants. Il nous faudra saisir toutes les chances de recruter les meilleurs.

Nous devrons enfin renforcer les liens et multiplier les interactions que nous avons avec nos partenaires industriels, de façon à développer un véritable écosystème Etat-industrie, capable d'intégrer les innovations de toutes parts pour être toujours plus efficace.

*

Et nous ne sommes plus au stade de la théorie. C'est une réalité qui prend corps, notamment dans **la Cyberdéfense factory que j'aurai l'honneur d'inaugurer tout à l'heure**, à quelques centaines de mètres d'ici. Cette antenne de l'Innovation Défense Lab est un espace unique qui accueillera des startups, des PME et des chercheurs pour travailler en étroite relation avec des experts de la Direction générale de l'armement sur des sujets de cybersécurité. C'est un lieu de partage des compétences mais aussi de partage des données : le Comcyber apportera aux acteurs de la Cyberdéfense Factory sa parfaite connaissance de l'environnement opérationnel, notamment dans l'élaboration et le partage de bases de données suffisamment représentatives de l'environnement opérationnel réel. Nous le savons, les spécialistes en intelligence artificielle le disent : l'accès aux données est un facteur décisif du succès.

La Cyberdéfense Factory n'a pas seulement vocation à capter les innovations du secteur civil. Car nous nous inscrivons dans cette démarche à double sens, un échange de bon procédés : car notre objectif est aussi que les entreprises bénéficient de l'expertise dont nous disposons en interne. Et c'est par ces échanges que nous favoriserons les innovations duales, utiles tant pour la société civile que pour le monde militaire. C'est ainsi que nos startups et nos PME pourront non seulement survivre, grandir mais aussi devenir des acteurs incontournables du marché européen, ou même du marché mondial. Notre objectif est aujourd'hui d'héberger une dizaine de projets innovants par an, puis, si l'expérience est fructueuse, de l'étendre à d'autres acteurs cyber, voire d'autres domaines.

La Cyberdéfense Factory fait partie d'une palette de nouveaux outils mis en place par la DGA pour lever les obstacles identifiés à l'occasion des deux défis cyber que nous avions récompensés lors du FIC 2019 : tout d'abord, le temps nécessaire à l'intégration des solutions innovantes dans les systèmes du Comcyber. Et ce temps est aujourd'hui trop long. Et comment pourrait-on accepter de devoir subir une attaque alors qu'une innovation disponible aurait permis de l'éviter ? Nous devrons nous montrer plus agiles pour rester dans le tempo du changement, et c'est toute la vocation de la Cyberdéfense Factory.

Le deuxième frein que nous souhaitons lever est celui du financement des startups, qui demeure limité et qui empêche les entreprises de croître et de développer de nouveaux produits. Leurs idées et leurs innovations sont précieuses et elles ne pourront devenir des succès que si elles sont financées abondamment et rapidement. C'est tout le message que le Président de la République a porté tout récemment à l'occasion du France Digitale Day.

Aujourd'hui, le ministère est un acteur engagé du financement des startups et des PME. Le dispositif RAPID a fêté ses 10 ans la semaine dernière. Ce sont entre 60 et 70 projets qui ont été financés et accompagnés dans le domaine du cyber grâce à RAPID, c'est un succès incontestable. Mais nous pouvons et nous devons voir plus grand.

Nous avons commencé à élargir nos horizons avec la création de Definvest, qui est un fonds d'investissement que nous avons lancé avec Bpifrance et qui nous permet d'investir plus massivement dans les entreprises à fort potentiel. Mais les entreprises ont aussi besoin du soutien et de la vitalité du financement des acteurs privés. C'est ce que nous souhaitons leur offrir en complément de ces outils et que nous leur offrons dès aujourd'hui. **Car j'ai le plaisir d'annoncer la signature d'une convention entre le ministère des Armées et la société d'investissement ACE Management pour accélérer les financements dans le domaine du cyber grâce à un fonds de 80 millions d'euros entièrement dédié à la cybersécurité**.

Ce fonds doit nous permettre de faire émerger de nouveaux acteurs du cyber et de consolider les existants pour les projeter à l'international. Ensemble, le fonds d'investissement et la Factory porteront cette ambition, l'une des plus belles et des plus enthousiasmantes, d'être une couveuse d'entreprises et de favoriser la création de startups.

Comme vous le voyez, les défis sont encore nombreux, et nous devrons être particulièrement sensibles aux enjeux de recrutements. Mais j'ai confiance en l'avenir. Nous sommes fidèles à nos promesses, fidèles à nos engagements, et nous sommes également fidèles à la loi de programmation militaire.

*

Une fabrique de champions cyber, voilà ce que nous créons aujourd'hui. Et vous serez ceux qui allez la porter. Vous êtes chercheurs, ingénieurs, techniciens et tous unis par cette même volonté d'exceller dans le cyber. Cette quête du sommet, cette ardeur à l'effort, c'est le moteur de notre défense. C'est avec cette énergie, avec votre expertise et vos talents que nous pourrons construire une cyberdéfense à la hauteur, pour développer et, quand il le faut, employer nos armes cyber offensives. Pour protéger nos systèmes, nos concitoyens et nos valeurs.

Le monde sait aujourd'hui qu'il faudra compter avec nous, dans le cyber, comme dans l'espace ou dans le champ de l'intelligence artificielle. Il le sait grâce à vous tous ; grâce à vous qui faites rayonner la France, vous qui faites de notre pays une cyber-puissance.

Vive la République ! Vive la France !