MINISTÈRE DES ARMÉES

Madame Florence Parly,

ministre des Armées

Stratégie cyber des Armées

Paris, le 18 janvier 2019

– seul le prononcé fait foi –

Mesdames et messieurs les élus,
Monsieur le chef d'état-major des armées,
Monsieur le délégué général pour l'armement,
Général,
Officiers, sous-officiers, militaires du rang,
Mesdames et messieurs,
Chers amis,

Des données volées. Des boîtes mails espionnées. Des serveurs pillés et des systèmes d'information enrayés.

Bienvenue en 2019. Bienvenue devant une réalité qui dès maintenant, pourrait entraver notre défense, briser nos secrets.

Le monde est connecté, vous le savez. Depuis le début de cette journée, vous avez regardé vos téléphones, consulté vos ordinateurs, utilisé vos mails. Moi, je l'ai fait. Depuis le début de la journée, nos forces aussi se sont appuyées sur des tablettes, des smartphones, des armes connectées. Elles ont reçu et transmis des ordres. Elles ont suivi et ciblé nos adversaires. Elles ont aussi échangé avec les leurs, avec leurs familles, peut-être.

Elles ont laissé autant de traces, autant de données. Elles ont partagé des informations et utilisé le numérique pour faire avancer notre sécurité.

Le numérique est un atout, bien sûr. Un atout que, par tous moyens, je veux saisir et développer. Mais c'est aussi un atout que nous devons domestiquer.

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.

Souvenons-nous. Souvenons-nous de TV5 Monde dont les écrans sont soudain devenus noirs et les comptes piratés. Souvenons-nous de WannaCry qui a touché 150 pays, touché des gares et des industries. Souvenons-nous, encore, il y a quelques jours, des milliers de données de la classe politique allemande piratées et révélées.

Tout est possible dans le cyberespace. Se pensant protégés par l'anonymat de leurs claviers, certaines personnes, certains groupes et certains Etats, 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.

Si des attaques ont pu porter atteinte à des infrastructures physiques, en Ukraine ou en Iran, elles n'ont pas encore réussi à provoquer des dommages massifs et durables à des économies et à des sociétés. Mais ce n'est sans doute qu'une question de temps. Et songez à la combinaison future d'attaques cyber et d'intelligence artificielle, se livrant à un combat sur les réseaux à une vitesse défiant toute compréhension humaine.

Et ces attaques cyber ne sont pas l'apanage du secteur civil. Nos systèmes militaires, eux aussi, sont épiés, visés, attaqués.

Il y a quelques mois, j'ai parlé d'espace. J'avais alors raconté l'histoire d'un satellite un peu indiscret. Laissez-moi aujourd'hui recommencer l'expérience.

Nous sommes fin 2017. Des connexions anormales sur le serveur de la messagerie internet du ministère des Armées sont constatées. Ces connexions ont révélé après analyse qu'un attaquant cherchait à accéder directement au contenu de boites mails de 19 cadres du ministère parmi elles, celles de quelques personnalités sensibles. Sans notre vigilance, c'est toute notre chaîne d'alimentation en carburant de la Marine nationale qui aurait été exposée.

Surtout, cette tentative d'attaque a duré jusqu'en avril 2018. Nous avons pu patiemment et, en étroite collaboration avec nos partenaires, remonter la chaîne des serveurs et des adresses IP Derrière se cachait un mode d'attaque bien connu de nos services et que certains attribuent à « Turla ».

En 2017, ce sont 700 événements de sécurité dont 100 attaques qui ont ciblé les réseaux du ministère. En 2018, ce même nombre a été atteint dès septembre. En moyenne, ce sont donc plus de deux événements de sécurité par jour qui ont touché tout autant notre ministère, nos opérations, nos expertises techniques et même un hôpital d'instruction des Armées. Certaines de ces attaques, directes, nous ciblaient précisément. D'autres, de côté, visaient nos industriels et nos partenaires.

Certaines sont le fruit de groupes malveillants. D'autres de hackers isolés. Mais certaines, nous le savons, viennent d'Etats pour le moins indiscrets, pour le moins… décomplexés.

Le cyber est une arme d'espionnage, bien sûr, mais elle est aussi une arme que des Etats 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.

Mesdames et messieurs, la France est en proie à suffisamment de menaces. N'y ajoutons pas notre propre naïveté. La guerre cyber a commencé et la France doit être prête à y combattre.

Nous le serons. Nous le serons en garantissant notre cyberdéfense, en protégeant mieux nos réseaux, nos systèmes et nos données. Nous le serons également en intégrant l'arme cyber dans nos opérations militaires.

Nous n'avons pas attendu, bien sûr. Nous avons étudié, expertisé. Nous avons déjà commencé à agir et affuter notre cyberdéfense.

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 maitrise 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.

Nous devons mieux anticiper les menaces et nous coordonner. La mise en place de nouvelles synergies et de partages entre les services de renseignement, le commandement de la cyberdéfense et la direction générale de l'armement répondent à ces impératifs.

Nous avons décidé d'organiser une chaîne cyber défensive « de bout en bout », qui protège autant nos forces que notre maintenance et notre industrie.

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.

Mais ce n'est pas tout : chaque entreprise, chaque partenaire du monde de la défense a son rôle à jouer.

Nos adversaires saisissent toutes les opportunités pour nous atteindre, cela implique bien sûr les industriels, leurs sous-traitants, leurs fournisseurs, leurs employés… Plus le ministère renforce ses pare-feu, plus les particuliers et les industriels sont visés. Chaque système d'arme, chaque ordinateur, chaque smartphone, et demain chaque objet connecté, peut, à l'insu même de son propriétaire, être non seulement une cible, mais un vecteur de cyberattaques.

Aussi, avons-nous décidé d'investir pour faire émerger une filière numérique de confiance, pour être capables de maîtriser le développement de nos innovations et l'emploi de nos solutions numériques. C'est l'un des objectifs de l'agence pour l'innovation défense tout juste créée, qui sera, sous l'égide de la DGA, notre bras armé pour mieux détecter et accompagner l'innovation. C'est l'un des objets de la hausse exceptionnelle des crédits pour la recherche et l'innovation. C'est l'une des raisons pour lesquelles nous croyons dans les PME et les start-up, car elles seront au cœur de notre réussite numérique.

La cybersécurité doit être prise en compte dès la conception dans chaque système d'arme, d'information et de communication. Il faut intégrer cette nécessité dans le besoin militaire et la rappeler, sans cesse, aux industriels. Je fonde beaucoup d'espoir sur le travail en plateau engagé entre l'EMA, les états-majors d'armées et la DGA. Le cyber doit être une de vos préoccupations majeures ; c'est d'autant plus nécessaire que le combat collaboratif sera au fondement de nos futurs systèmes d'arme. C'est déjà le cas et cela le sera encore plus avec l'arrivée de programmes majeurs comme SCORPION, le système de combat aérien futur ou encore le porte-avions de nouvelle génération, dont nous savons tous qu'ils tireront leur efficacité opérationnelle de leur capacité à agir en réseau.

Le ministère des Armées et les entreprises doivent travailler ensemble, se comprendre et se préparer. Nous devons adapter nos méthodes de travail, notre culture, partager les bonnes pratiques, qui évitent des failles béantes. L'« hygiène cyber » n'est pas un luxe, c'est une absolue nécessité pour nos systèmes d'armes et ceci tout au long de leur vie, de leur conception technique à leur emploi opérationnel.

C'est pourquoi la semaine prochaine, au Forum international de la cybersécurité, je proposerai un partenariat entre le ministère et les grands industriels de défense qui liera industries de défense, la DGA et le COMCYBER en fondant ce dispositif de cyberdéfense de « bout en bout ». L'objectif est simple : toute notre communauté de défense doit se protéger et être protégée.

Vous l'aurez compris, il faut éviter de tendre la joue. Il faut également préparer nos armées à cette nouvelle guerre, en nous assurant qu'elles disposent d'une doctrine et de capacités de lutte informatique offensive.

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.

Mais nous serons aussi prêts à employer en opérations extérieures l'arme cyber à des fins offensives, isolément ou en appui de nos moyens conventionnels, pour en démultiplier les effets.

Je veux que cette utilisation des outils cyberoffensifs par nos armées se fasse dans le plus strict respect des normes du droit international public. Notre processus de ciblage numérique est extrêmement strict. Il nous permet de respecter les principes de proportionnalité, de distinction et de nécessité. Dans l'esprit de l'appel de Paris, nous respecterons le droit international, bien sûr, et les cybercombattants bénéficieront des mêmes protections que les militaires en OPEX.

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.

La cyberdéfense demande des compétences de haut niveau, souvent rares. Le métier de combattant numérique est récent : il y a 15 ans à peine, on aurait probablement cru à une utopie. Et pourtant, il existe bel et bien. Il lie expertise technique, finesse d'analyse et « savoir-être » militaire.

Il nous faut donc une politique RH ambitieuse, attractive et adaptée aux jeunes talents que nous voulons recruter et conserver. Nous ne devons nous fermer aucune porte et envisager des filières de formation, d'entraînement et de recrutement tout à fait nouvelles. Je le dis avec une certaine fierté, les armées, la DGA et la DGSE disposent de compétences dans le domaine. Leur mise en œuvre et leur développement nécessitent de jeunes talents. Ils sont les bienvenus !

Nous devons assumer l'intégration pleine et entière des outils cyber au sein de la palette opérationnelle de nos armées. Leurs effets doivent être connus, leur emploi parfaitement maîtrisé et encadré. Nos adversaires potentiels doivent savoir à quoi s'attendre. C'est pourquoi j'ai décidé de rendre publics les grands principes de notre doctrine de lutte informatique offensive à des fins militaires, tout en protégeant naturellement les éléments les plus sensibles. C'est une condition nécessaire pour garder toute notre supériorité sur les théâtres d'opérations.

Dans ce nouvel espace de confrontation, la France n'est donc pas naïve et elle assume le conflit potentiel, dans le plein respect de ses engagements internationaux. Je veux le dire aussi, elle restera fidèle à sa tradition et continuera d'être à l'initiative pour proposer des normes de comportement responsable et garantir, au maximum, la stabilité stratégique dans le cyberespace.

Monsieur le chef d'état-major des Armées, j'ai présenté le cadre de notre doctrine de lutte informatique offensive et je vous laisserai dans quelques minutes le soin de la préciser plus en détail.

Mesdames et messieurs, le Président de la République m'a fixé un mandat clair : protéger les Français. Les protéger des menaces et des attaques. Les protéger, aussi, des conflits qui guettent, des capacités qui se créent.

Depuis 18 mois, j'ai donc un but : bâtir les Armées du XXI^{e} siècle. Et aujourd'hui, nous avons franchi une nouvelle étape, forte, déterminante pour la défense de tous les Français.

Aujourd'hui, nous refusons le conservatisme qui voit le numérique comme une mode et la naïveté de ceux qui le regarde avec béatitude, sans en comprendre les dangers.

Aujourd'hui, nous envoyons un message ferme à nos adversaires et nous tendons la main à nos alliés.

Aujourd'hui, nous nous dotons d'un cadre clair et nous l'assumons : oui, la France emploie et emploiera l'arme cyber dans ses opérations militaires.

Vive la République ! Vive la France !