M. Jean-Yves Le Drian, Ministre de la Défense

Discours d'annonce du pacte « Défense cyber 2016 »

A l'école des transmissions, vendredi 7 février 2014

– Seul le prononcé fait foi –

Mesdames, Messieurs les élus,

Monsieur le délégué,

Messieurs les officiers généraux,

Mesdames, Messieurs les officiers,

Mesdames et Messieurs,

Je suis très heureux de vous retrouver ce matin. Les quarante ans de l'école des Transmissions nous avaient réunis une première fois en juin dernier ; la cyberdéfense était déjà à l'ordre du jour. Aujourd'hui, elle l'est plus que jamais.

La cyberdéfense est l'une des deux priorités nationales fixées par le livre blanc de 2013. Derrière elle, il y a des menaces dont la gravité est réelle. Quelques chiffres permettent d'en prendre la mesure. Pour m'en tenir au ministère dont j'ai la charge, en 2013, nous avons dû affronter plus de 780 incidents informatiques significatifs, contre 420 en 2012. Si ces chiffres résultent d'une augmentation de notre niveau de vigilance et d'une meilleure surveillance, ils témoignent aussi de la croissance exponentielle de la menace en provenance du cyberespace, sous des formes qui sont de plus en plus variées, de plus en plus complexes et de plus en plus diffuses.

C'est une priorité pour le ministère de la défense, car notre efficacité opérationnelle, notre capacité même à conduire des opérations, peut être gravement affectée par la menace cyber. Je pense ici aux systèmes d'armes, aux systèmes de commandement, d'information et de communication qui les relient, mais aussi à tous les systèmes logistiques ou industriels qui les soutiennent.

C'est une priorité pour mon ministère, car toute opération militaire comporte désormais un volet cyber plus ou moins développé. Nous l'avons vu dans l'affrontement entre la Géorgie et la Russie en 2008. Nous le voyons dans la place croissante qu'occupe le cyber dans les arsenaux des nations. La réussite de ces opérations dépend donc aussi, de plus en plus, de la prise en compte de ce nouveau champ stratégique.

C'est une priorité pour la Défense nationale car, même si des progrès ont été accomplis depuis le livre blanc de 2008, de nombreux efforts restent à fournir, en termes de formation, de recherche, de sensibilisation… C'est tout l'objet de ma présence aujourd'hui, je vais y revenir.

Définir ce nouveau domaine stratégique comme une priorité, ce n'est donc pas simplement affirmer une posture. C'est une ambition que nous incarnons à travers des mesures très concrètes, qui

doivent profiter au ministère de la défense, mais également à l'ensemble de la communauté nationale de cybersécurité.

C'est ensemble que nous allons intensifier l'effort pour relever ce défi stratégique de grande ampleur.

A l'occasion du Forum International de la Cybersécurité, qui s'est tenu récemment à Lille, j'ai annoncé la mise en place prochaine d'un pacte sur la cyberdéfense. Je viens aujourd'hui dans ce lieu symbolique pour lancer officiellement ce pacte que j'ai souhaité intituler pacte « défense cyber 2016 ».

2016, d'abord, parce que je veux des résultats rapides. Bien sûr, l'effort du ministère de la défense s'étendra au-delà de 2016, et il a vocation à porter des effets pérennes. Mais 2016 est l'année où la loi de programmation militaire arrivera à mi-période, et fera donc l'objet, comme je m'y suis engagé d'un réexamen approfondi. Ce sera le moment opportun pour faire le bilan de l'action menée en matière de cyberdéfense, d'autant que ce domaine est particulièrement évolutif. Notre action s'inscrit dans le temps long, mais nous devrons l'ajuster régulièrement.

Ce pacte « défense cyber 2016 » embrasse donc tous les aspects de la cyberdéfense. Il inclut notamment les projets liés au pôle d'excellence cyber en Bretagne. A travers six axes d'effort, il recense toutes les actions à conduire sur la première période de la LPM – c'est-à-dire les années 2014 à 2016.

Comme le pacte « défense PME », il est constitué d'un ensemble de mesures très concrètes, cinquante exactement, qui vont être mises en œuvre dans le périmètre du ministère dont j'ai la charge, pour garantir un niveau élevé de cybersécurité, au plan notamment de l'anticipation, de la réactivité et de l'expertise.

Mais ce pacte « défense cyber 2016 », c'est aussi une main tendue vers toute la communauté nationale de cyberdéfense. Si nous voulons que la France reste dans le cercle des nations qui comptent dans le cyberespace, le ministère de la défense doit en effet mettre son excellence et ses capacités au service de la posture nationale de cybersécurité. Il doit le faire en bonne intelligence avec l'ANSSI et les autres ministères régaliens, et en premier lieu avec le ministère de l'intérieur, qui a la charge de la lutte contre la cybercriminalité et se trouve particulièrement impliqué dans la gestion des crises sur le territoire national.

Ce pacte repose sur une démarche pragmatique, avec toute une série de projets concrets organisés selon six axes d'efforts que je vais vous présenter dans leurs grandes lignes. Ensemble, ils représentent un effort d'un milliard d'euros sur la durée de la loi de programmation militaire.

Le premier axe vise à renforcer le niveau de sécurité des systèmes d'information, ainsi que les moyens de défense et d'intervention du ministère et de ses premiers partenaires.

Le ministère dont j'ai la charge doit garantir le fonctionnement et la défense des systèmes dont il a la responsabilité, tant sur le territoire national qu'en dehors de nos frontières. Cela passe,

concrètement, par le développement et l'utilisation de moyens permettant de maintenir notre autonomie, par exemple des équipements et des logiciels souverains.

Nous allons ensuite améliorer notre organisation interne, en renforçant la chaîne opérationnelle de cyberdéfense autour du CALID. Ce centre verra ses effectifs multipliés par 6 d'ici 2019, par rapport à 2011, et nous créerons une entité CALID Bretagne en 2016.

Le développement d'un renseignement d'intérêt cyber, en lien avec tous les acteurs du renseignement du ministère, relève également de cet axe. Il contribue en effet à renforcer notre posture de cyberdéfense, en anticipant et évaluant la menace cyber.

Pour la première fois, le cadre juridique de la cyberdéfense a été défini par le législateur dans le cadre de la LPM, sur des bases claires et novatrices. Je pense à la définition des pouvoirs réglementaires du Premier ministre. Je pense aux obligations imposées aux opérateurs d'importance vitales. Je pense encore à la capacité à se défendre et à riposter dans le cyberespace.

Mon ministère, enfin, doit poursuivre ses efforts pour préciser le cadre juridique de la cyberdéfense spécifique aux armées pour garantir l'efficacité de nos forces. Une dizaine de juristes spécialisés seront ainsi placés au sein de la direction des affaires juridiques et au profit des entités opérationnelles.

Concernant le deuxième axe, il vise à préparer l'avenir en intensifiant l'effort de recherche, aux plans technique, académique mais aussi opérationnel, tout en apportant un soutien à notre base industrielle.

Ici, nous devons encourager les étudiants et les centres de recherches qui s'investissent dans le domaine de la cyberdéfense, par exemple en soutenant plus de doctorats, que ce soit à travers la DGA ou l'IRSEM. Nous allons ainsi doubler le nombre de thèses consacrées à la cyberdéfense et soutenues par le ministère. La création en 2012 de la chaire de cyberdéfense en partenariat avec les Ecoles de Saint-Cyr Coëtquidan et des entreprises privées, marque la volonté du ministère d'inscrire cet effort sur le long terme. D'autres chaires verront le jour d'ici 2015, notamment à l'Ecole navale à Lanvéoc-Poulmic, et à l'Ecole de l'air.

Nous allons par ailleurs tripler le montant des études amont dans ce domaine, car il est indispensable de disposer d'une base industrielle adaptée à nos enjeux de souveraineté. Nous augmenterons d'ailleurs la part de projets dédiés au cyber au sein du dispositif RAPID de soutien aux PME/PMI, sans rogner sur les autres projets, puisque l'ensemble du dispositif augmente lui-même de 25% dès le début de la LPM.

Le ministère de la Défense doit enfin contribuer à l'approfondissement d'une pensée stratégique et opérationnelle française en matière de cyberdéfense. Ici, au-delà même des chercheurs que nous soutenons, nous devons accroître les échanges que nous avons avec nos partenaires étrangers, pour confronter nos idées et ainsi faire progresser la réflexion française.

Le troisième axe concerne particulièrement l'Ecole des Transmissions, puisqu'il s'agit de la formation.

Le domaine cyber, d'un point de vue technique, est extrêmement complexe. Il suppose des personnels toujours à la pointe, sous l'angle technologique et opérationnel. Ces ressources humaines sont rares, et donc fortement demandées. Nous devons en tenir compte. Pour ce faire, nous devons d'abord identifier les profils les plus adaptés aux missions et aux exigences du ministère. C'est un travail délicat qui repose sur de nombreux réseaux professionnels. A ces personnes nous devons proposer des parcours professionnels attractifs. Le ministère offre ici un cadre très appréciable, dans la lutte informatique défensive sur le territoire, sur des théâtres d'opération, jusqu'aux actions offensives les plus élaborées. Ces parcours peuvent – et je dirais même qu'ils doivent – reposer sur des échanges croisés avec les autres ministères, le monde de la recherche académique et l'industrie. Nous avons tout à gagner d'une fertilisation croisée. Enfin, nous devrons former ces personnels en permanence, afin qu'ils demeurent au niveau le plus élevé.

Le quatrième axe concerne le développement d'un pôle d'excellence en cyberdéfense, ici même en Bretagne.

L'école des Transmissions est déjà un exemple pour ce pôle: école de l'Armée de terre, elle met ses locaux et son expertise au service de la formation de près de 3600 stagiaires par an. Ses stagiaires sont des militaires ou des civils, qui viennent de l'armée de Terre bien sûr, mais aussi de la Marine et de l'Armée de l'air, ainsi que des directions et services du ministère. Ouverte à l'international, l'ETRS forme également 70 stagiaires étrangers venant de pays amis de la France. Elle est par ailleurs particulièrement bien implantée dans son environnement proche, avec d'ores et déjà des liens forts qui l'unissent à d'autres organismes de formation de la région.

Ce pôle se structurera autour de trois composantes qui s'appuieront mutuellement : la première, consacrée à la formation, doit fournir une ressource humaine qualifiée pour armer les différents organismes techniques ou opérationnels du ministère ; la deuxième, tournée vers la recherche et le développement, doit garantir la capacité de notre industrie à concevoir et développer les produits et services dont nous avons besoin dans la durée ; la troisième, enfin, sera à vocation opérationnelle, notamment pour les investigations les plus pointues et la projection de capacité de protection ou d'intervention.

L'échelon précurseur de ce pôle sera composé des centres d'expertise et écoles du ministère dans la région. Je pense à DGA Maîtrise de l'information, aux Ecoles de saint-Cyr Coëtquidan, à l'Ecole Navale, à l'ENSTA Bretagne, et bien évidemment, à l'Ecole des transmissions. Il s'appuiera également sur les partenariats qui se sont déjà noués avec les établissements d'enseignement supérieur et les laboratoires de la région dans les domaines concourant à la cyberdéfense.

Ces partenariats pourront conduire à mettre en commun les expertises, les expériences et les capacités. Je pense en particulier à la plateforme de simulation distribuée que nous sommes en train de déployer.

Ces efforts de formation et de recherche devront également profiter au tissu industriel local, les grands groupes comme les PME/PMI, au travers de financement de thèses et de projets.

Pour illustrer cet effort de formation, je suis en mesure de vous annoncer qu'ici même, au sein de l'Ecole des Transmissions, en coopération avec les Ecoles de Saint Cyr Coëtquidan, un mastère

spécialisé en conduite des opérations et gestion des crises cyber sera mis en place à la rentrée 2015. Ce mastère donnera une compréhension globale des enjeux du cyber : techniques, éthiques, juridiques et opérationnels. Il formera également à la gestion de crises. Il sera d'abord destiné aux cadres militaires des différentes armées qui auront à exercer des responsabilités au sein du ministère. Mais il sera également ouvert à notre personnel civil, puis à celui des autres administrations ou organismes d'intérêt vital, et enfin à certains de nos partenaires étrangers. Ce mastère, qui est sans équivalent, accompagne la consolidation de l'ensemble des autres formations techniques dispensées aux officiers et aux sous-officiers en sécurité des systèmes d'information et en lutte informatique défensive.

J'en viens au cinquième axe qui concerne nos relations avec nos partenaires étrangers, que ce soit en Europe, avec l'OTAN ou dans des zones d'intérêt stratégique, notamment au Moyen-Orient ou dans le Pacifique.

Pour assurer la cyberdéfense de nos forces et plus largement de notre territoire, nous devons bâtir des coopérations qui nous permetttent d'échanger des informations, et éventuellement de coordonner nos actions dans le cyberespace. Ces efforts de coopération viendront appuyer les actions entreprises par le ministère des affaires étrangères et l'ANSSI.

Le sixième et dernier axe de ce pacte défense cyber 2016 est peut-être le plus important, puisqu'il vise à faire émerger une communauté nationale de cyberdéfense.

Il résume le pacte. Afin de mettre en œuvre les cinquante mesures proposées, nous devons être en mesure de travailler au sein d'une même communauté, pour nous saisir d'un enjeu qui est global et transverse à la fois. L'émergence d'une communauté nationale de cyberdéfense, qui se fonde sur des relations de confiance, constitue le socle essentiel de toutes nos actions. Cette communauté pourra également s'appuyer sur un cercle de partenaires et sur les réseaux de la réserve cyberdéfense, présents jusque dans les régions. J'en profite pour saluer les actions menées par le réseau cyberdéfense de la réserve citoyenne de Bretagne. Ce réseau, composé de réservistes citoyens, bénévoles du service public, vient apporter son soutien aux acteurs locaux, notamment dans leurs démarches de sensibilisation auprès des entreprises, des collectivités locales et des écoles. Cette démarche est également essentielle.

Mesdames et Messieurs,

Depuis plusieurs mois, à travers le livre blanc puis la loi de programmation militaire, le ministère de la défense est porteur d'une ambition de premier ordre dans le domaine de la cyberdéfense. Cette ambition se décline aujourd'hui à travers un plan d'un milliard d'euros, qui va contribuer de manière décisive à la préservation de notre autonomie stratégique.

Le ministère dont j'ai la charge assume plus que jamais le rôle qui doit être le sien. Il le fait en lien avec tous les autres acteurs de la communauté nationale de cyberdéfense. Au moment d'engager un effort sans précédent dans ce domaine, il réaffirme que c'est collectivement que nous nous montrerons à la hauteur des menaces du cyberespace.

Je vous remercie.