MINISTÈRE DE LA DÉFENSE

M. Jean-Yves Le Drian,

Ministre de la défense

Discours d'ouverture du colloque sur la cyberdéfense

A Rennes, lundi 3 juin 2013

– Seul le prononcé fait foi –

I) Introduction

Monsieur le Président, cher Pierrick,
Messieurs les officiers généraux,
Mesdames et Messieurs,

Je suis très heureux d'être avec vous ce matin, pour ouvrir ce colloque sur la cyberdéfense. Au moment où l'Ecole des transmissions fête ses quarante ans, c'est une grande satisfaction que de la voir se tourner ainsi vers l'avenir. Et notre plaisir est vif de voir, dans le même mouvement, la région Bretagne se distinguer par son excellence dans le domaine de la cyberdéfense.

II) Cybersécurité et livre blanc : le contexte

a) Le cyber espace : riche d'opportunités mais lourd de menaces

La cyberdéfense est une nouvelle donne stratégique. C'est d'abord un nouvel espace, riche d'opportunités mais aussi lourd de risques et de menaces. C'est ensuite un champ de recherche et d'action qui dépasse en effet les schémas classiques et qui nous incite à repenser globalement certains de nos modes de fonctionnement. Le Livre blanc sur la défense et la sécurité nationale, que le Président de la République vient d'approuver, prend toute la mesure de cette nouvelle

donne stratégique. En la considérant dans sa globalité, il porte la cybersécurité au rang de priorité nationale. Le mouvement initié par le Livre blanc de 2008 est donc accéléré ; un cap ambitieux est désormais fixé.

b) Un enjeu sous-estimé : un effort considérable est nécessaire afin de sécuriser les systèmes d'importance vitale de la nation

Le constat est simple. L'interconnexion des systèmes d'information qui marque notre société, a généré des vulnérabilités nouvelles, qui n'ont pas été suffisamment accompagnées d'un effort simultané de protection. Les atteintes aux systèmes d'informations résultant d'actes hostiles intentionnels ou de ruptures accidentelles pourraient dès lors engendrer des dysfonctionnements, voire une paralysie de l'Etat ou de secteurs d'importance vitale pour la Nation. Je crois qu'il faut le reconnaître. Avons-nous été naïfs, trop confiants dans le développement de l'Internet et, plus largement, des systèmes d'information ? Comprendre le caractère stratégique de cet enjeu, reconnaître sa globalité est un défi majeur, que certains de nos grands partenaires ont bien compris.

Le temps passe et les évolutions s'accélèrent. L'hypothèse d'attaques informatiques majeures s'est renforcée depuis 2008, et le cyberespace est devenu un champ de confrontations à part entière. A titre d'exemple, le nombre d'attaques traitées par le ministère de la

Défense, à travers le centre CALID, est en très forte augmentation : 420 en 2012, contre 196 en 2011.

L'enjeu n'est plus seulement le risque de déni d'accès ou de pénétration des réseaux à des fins d'espionnage, alors même que ce risque est déjà considérable et avéré. Ce qui est désormais en jeu, c'est la capacité de prise de contrôle à distance ou bien de destruction d'infrastructures vitales pour notre pays, reposant sur des réseaux numérisés ; c'est désormais l'atteinte aux intérêts stratégiques de l'Etat et à notre autonomie d'appréciation, de décision et d'action, par la menace cyber. C'est un enjeu majeur de défense et de souveraineté de la Nation.

Au-delà de la dépendance accrue de la Nation aux systèmes d'information, les cyberattaques constituent donc, dès aujourd'hui et plus encore à l'horizon du Livre blanc, une menace majeure, à forte probabilité et à fort impact potentiel. De fait, chaque nouveau conflit comporte un volet cybersécurité, qui est de plus en plus global : il touche aussi bien les individus, comme au début des révolutions arabes, que le cœur d'un sanctuaire national avec l'épisode Stuxnet en Iran, ou encore des acteurs économiques majeurs, comme l'illustrent les attaques de l'été 2012 contre la société Aramco, le principal exportateur saoudien.

Mais le cyber est aussi investi par des groupes non étatiques, qui y trouvent une arme idéale. Que leurs motivations soient politiques, idéologiques ou mafieuses, ils développent ainsi la capacité d'affronter à distance un Etat, avec une facilité qui leur était auparavant interdite. Bien plus, l'ordre international qui fixe les frontières et régit les rapports entre les Etats, se retourne à l'avantage de ces groupes en gênant les poursuites contre eux, par une série d'obstacles juridiques et politiques qui, pour l'heure, n'ont pas été levés.

c) Ne peut que s'appréhender en multinational (union européenne et OTAN)

Ce défi majeur, chaque nation européenne y fait face aujourd'hui ; chacune en est consciente et développe ses propres stratégies ; mais pour peser, je veux le dire d'entrée, la solution, notre solution, ne peut être qu'européenne. Je salue les efforts récents de l'Union Européenne pour se doter d'une stratégie en la matière. C'est une première étape. La prochaine, avec un Conseil européen en décembre consacré aux questions de défense, devra approfondir cette ambition. Il appartient aux Européens de prendre en charge leurs propres infrastructures vitales ; il leur revient de trouver une juste complémentarité avec l'OTAN. De ce point de vue, il faut valoriser les centres d'excellence dont ces organisations disposent d'ores et déjà. Je pense notamment au centre de Tallinn, en Estonie, pays qui fut la première victime

d’une attaque cybernétique de grande ampleur. C’était en 2007. Aujourd’hui, la France rallie ce centre avec une volonté, celle de rapprocher l’Union et l’Alliance dans le domaine de la cyberdéfense.

III) Cybersécurité et livre blanc : la réponse

a) Le Livre Blanc 2013 précise la doctrine nationale qui associe prévention et réaction

Pour cet ensemble de raisons, le Livre blanc de 2013 élabore une doctrine nationale de réponse aux agressions informatiques majeures. Une politique de sécurité ambitieuse sera ainsi mise en œuvre, afin d’identifier l’origine des attaques, d’évaluer les capacités offensives des adversaires potentiels et l’architecture de leurs systèmes, et de pouvoir ainsi les contrer. Cette politique sera globale, avec deux volets complémentaires.

D’une part, la montée en puissance d’une posture robuste et résiliente pour protéger les systèmes d’information de l’État, les opérateurs d’importance vitale et les industries stratégiques. Cette posture repose sur une organisation opérationnelle de défense de ces systèmes, qui est coordonnée sous l’autorité du Premier ministre et qui associe étroitement les différents services de l’Etat. C’est le premier volet.

D’autre part, une capacité de réponse gouvernementale devant des agressions qui sont de nature et d’ampleur variées. Cette capacité de réponse fera en premier lieu appel à l’ensemble des moyens diplomatiques, juridiques ou policiers, sans s’interdire l’emploi gradué de moyens relevant du ministère de la défense, si les intérêts stratégiques nationaux sont menacés.

Pour atteindre ces objectifs, plusieurs axes d’effort ont été identifiés, et vous me permettrez d’en dire un mot.

b) Une capacité offensive viendra compléter les moyens d’action de l’Etat

En premier lieu, au sein de cette doctrine nationale, la capacité informatique offensive, associée à des capacités de renseignement, concourt de façon significative à notre posture de cybersécurité. Elle contribue notamment à caractériser la menace et à identifier son origine. Elle permet, en outre, d’anticiper certaines attaques et de configurer nos moyens de défense en conséquence. La capacité offensive enrichit la palette des options qui sont à la disposition de l’Etat. Elle comporte elle-même différents stades, qui sont plus ou moins réversibles, plus ou moins discrets, mais toujours proportionnés à l’ampleur et à la gravité de la situation.

c) Plus spécifiquement au sein du Ministère de la Défense, la posture de cybersécurité monte en puissance et concerne l'ensemble des milieux classiques (terre, air, mer)

La démarche est donc globale, mais elle concerne spécifiquement la défense, et je voudrais à présent m'y attarder. Le nouveau modèle d'armée comprend des capacités de cyberdéfense militaire, en relation étroite, d'abord, avec le domaine du renseignement. Dans le cyberespace en particulier, où les frontières sont floutées et où le brouillard du monde virtuel permet toute sorte de manipulation, le renseignement joue en effet un rôle majeur, pour connaître et anticiper la menace. Dans ce contexte, on comprend que l'imputation des attaques ne saurait se limiter à des preuves de nature juridique, mais doit intégrer l'intime conviction que permettent des faisceaux d'indices convergents.

Ces dernières années, des attaques ont pour la première fois explicitement visé la neutralisation de systèmes critiques, même non connectés à Internet. Ces attaques sont de plus en plus sophistiquées et ciblées. Outre la protection des informations, la fiabilité et la résilience des systèmes d'armes comme des porteurs représentent donc aujourd'hui un enjeu majeur pour nos armées. De nombreuses mesures ont été déjà prises, à la fois pour fortement renforcer notre posture de cybersécurité, qui repose sur un volet préventif de

protection et un volet actif de défense des systèmes, mais aussi pour développer une capacité offensive.

Ainsi, les moyens humains qui sont consacrés à la cyberdéfense seront sensiblement renforcés, à la hauteur des efforts consentis par nos principaux partenaires européens. Ils vont ainsi augmenter de 350 personnes d'ici 2019. Ensuite, un renforcement de la sécurité des systèmes d'information de l'État est nécessaire. Au-delà, l'État doit soutenir les compétences scientifiques et technologiques performantes du domaine cyber, car la capacité à produire en toute autonomie nos dispositifs de sécurité, notamment en matière de cryptologie et de détection d'attaque, est une composante essentielle de la souveraineté nationale. Enfin, le développement de relations étroites avec nos principaux partenaires étrangers devra être soutenu.

d) La chaîne opérationnelle de commandement intègrera dorénavant l'ensemble des aspects cyber

Vous comprenez ainsi que le cyberespace est désormais considéré comme un milieu à part entière par les armées ; il fait l'objet d'une approche semblable à celle adoptée pour les milieux aérien, terrestre et maritime. Une chaine de commandement opérationnel de la cyberdéfense est ainsi déployée depuis 2011. Pleinement intégrée au commandement interarmées des opérations, elle traite de l'ensemble

des volets de la cyberdéfense. Un schéma directeur, à l'horizon 2020, a été réalisé et validé il y a un an.

Cette chaine opérationnelle de cyberdéfense est donc en voie de consolidation. Elle permettra d'offrir une vision globale et une mobilisation rapide des moyens en cas de besoin, tout en s'intégrant pleinement aux autres chaines de conduite des opérations maritimes, aériennes, terrestre ou spéciales. Car il ne s'agit pas de greffer un nouveau service qui serait autonome, mais au contraire d'irriguer, sous un commandement unifié, l'ensemble des actions menées. Le cyberespace est partout ; il est consubstantiel des autres milieux. L'enjeu est donc de travailler autrement, d'adapter la façon de commander, de coopérer étroitement, et le cas échéant de mutualiser les équipements. C'est dans cette logique que les centres de surveillance relevant de l'ANSSI et de la chaine cyber des armées seront co-localisés à partir de cet été. Dans le même esprit de rapprochement des acteurs et des modes de travail, des experts opérationnels des armées sont d'ores et déjà intégrés au sein des équipes techniques de la DGA, pour bénéficier d'une boucle très courte entre les besoins opérationnels et l'expertise technique.

Au-delà de cette organisation, une nouvelle doctrine de cyberdéfense militaire est en préparation, dix-huit mois après la précédente. C'est dire si cette nouvelle donne stratégique évolue rapidement, et combien nous devons nous-mêmes savoir nous y adapter.

e) La base industrielle (grands groupes et PME) sera renforcée par un soutien à la R&D et la mise en place d'une politique industrielle coordonnée

Dans la même perspective, le renforcement de la base industrielle de technologies de défense et de sécurité nationale est indispensable, car elle demeure fragile, malgré un véritable potentiel. La cybersécurité est une question de spécialistes, mais elle est en même temps l'affaire de tous, et je pense ici en particulier aux acteurs économiques. Nous bénéficions de la présence en France de grands industriels de défense, capables de réaliser des systèmes complexes et performants, ainsi que de grands opérateurs. Nous disposons également de nombreuses PME innovantes, que nous devons soutenir et protéger. Mais il faut encore accroître notre effort et développer les synergies.

A cette fin, une politique industrielle est en cours d'élaboration, depuis le financement de la R&D au soutien à l'exportation, en passant par d'importants programmes d'équipement en moyens de cyberdéfense et de sécurisation de nos grands systèmes d'information. Ce ne sont pas seulement des mots : les crédits consacrés aux études amont sont en train d'être triplés, de 10 à 30M€ par an. Ces études sont cruciales ; en levant des verrous technologiques, et en développant des compétences techniques très pointues au sein des équipes étatiques et industrielles, elles préparent l'avenir à court,

moyen et long terme. Pour compléter cette politique, la recherche académique est encouragée, notamment au travers de contrats d'étude et de co-financement de thèses de doctorat.

f) La réserve citoyenne et opérationnelle doit être développée

Elaboration d'une doctrine, renforcement de la chaîne de commandement opérationnelle, définition d'une politique industrielle… Le développement de nos capacités militaires de cyberdéfense s'insère dans une démarche globale, qui doit faire l'objet d'une haute priorité, pour rester en phase avec la croissance très rapide de la menace que j'évoquais il y a un instant.

Cet effort considérable que nous devons fournir, pour ne pas nous laisser distancer, reposera avant tout sur les hommes et les femmes qui vont être les acteurs de la cybersécurité de notre société numérique. C'est toute la question de la réserve. A côté de la réserve citoyenne qui a été créée pour sensibiliser la société à ces problématiques et créer un esprit de cyberdéfense, il semble important d'étudier la mise en place d'une réserve opérationnelle, qui serait adaptée à traiter une crise informatique majeure touchant l'ensemble du territoire, cela en appui des différents services de l'Etat et des collectivités territoriales.

IV) Cybersécurité et Bretagne

Mais c'est aussi et surtout vers la formation que notre effort doit se porter, et j'en viens aux lieux qui nous rassemblent aujourd'hui.

a) La formation est un sujet majeur qui doit se développer notamment en Bretagne autour de Coëtquidan avec la participation des acteurs étatiques, académiques et industriels

Avec plusieurs grands partenaires du monde des technologies de l'information, le ministère de la défense soutient l'idée d'un pôle d'excellence de cyberdéfense. Ce pôle pourrait se traduire par un projet ambitieux, avec un centre de cyberdéfense associant les compétences des armées et de la DGA, à celles des écoles d'ingénieurs (SUPELEC, TELECOM Bretagne…) et des grands centres universitaires de la région (Rennes II, IUT Lannion et Saint-Malo, ou encore l'Université de Bretagne Sud avec la mise en place d'une formation originale par alternance en apprentissage). Cet ensemble bénéficierait de l'image des Ecoles de Saint-Cyr Coëtquidan, autant que du soutien avisé des grands maîtres d'œuvre des systèmes de défense.

Vous l'aurez deviné, c'est là une vision qui me tient à cœur. Elle porte certes une part d'inconnues, mais devant la multiplication des enjeux cyber, je crois qu'il devient urgent d'être ambitieux. Coëtquidan, où la

première chaire de cyberdéfense et cybersécurité a été inauguré en novembre 2012 en partenariat avec Sogeti et Thalès, est le creuset où peut se forger cette capacité dont notre nation a besoin. La DGA soutiendra la démarche en apportant son expertise technique en termes de connaissance de la menace, de maîtrise et de simulation des systèmes complexes. L'Ecole des transmissions sera également fortement associée, en particulier dans le cadre de la formation à la technique, aux modes opératoires et aux doctrines, mais aussi à l'éthique, qui est un autre enjeu essentiel dans un espace où la technologie permet toutes les manipulations.

C'est une aventure audacieuse, une vision à laquelle il convient de donner vie. Tous les ingrédients sont réunis pour que la Bretagne accueille ce projet de centre de formation à la cyberdéfense, et j'appelle dans cette perspective nos grands partenaires à rejoindre l'élan qui est déjà celui de nos amis de la communauté de communes du pays de Guer. J'ai d'ailleurs, dans cette perspective, missionné l'inspecteur général des armées-armement Jean-Bernard Pène, pour montrer la faisabilité académique et la viabilité économique de ce projet et, du même coup, engager un dialogue avec tous les acteurs intéressés – les écoles, la DGA, les laboratoires, les entreprises… La constitution d'un club de partenaires me semble à cet égard une perspective intéressante.

Mais nous ne devons pas seulement nous cantonner à la formation d'experts et de techniciens. Un effort de sensibilisation doit être fait à l'égard des collégiens et des lycéens, et là encore, la région Bretagne, à travers son projet Bretagne numérique, a un rôle à jouer.

Enfin et surtout, l'activité dans ce domaine doit se nourrir de collaborations avec tous les acteurs comme les écoles, la DGA, les laboratoires des universités, les entreprises.

b) Le soutien à l'innovation est l'autre priorité, notamment à destination des PME, et particulièrement en Bretagne

A côté de la formation, une autre urgence concerne le développement et l'innovation, qu'il faut encourager. Nous le faisons, et c'est notre force. Mais il y a une difficulté, qui tient un peu de la lutte entre glaive et le bouclier. L'enjeu est d'un côté de savoir détecter les attaques qui visent les systèmes d'information, et de l'autre côté, de rester en capacité de fournir le système le plus robuste possible, cela au meilleur rapport coût-efficacité. Cet équilibre n'est pas simple à trouver. Dans ce domaine de l'innovation, deux acteurs se distinguent au profit de la cyberdéfense, et je veux les saluer : les opérateurs, ou systémiers, qui sont les seuls à maîtriser de bout en bout la complexité croissante de la mise en œuvre des réseaux et des grands systèmes, mais également les PME, nombreuses dans notre région, qui

constituent ensemble un creuset sans pareil de l'innovation technologique.

Dans ce domaine également, la Bretagne est appelée à jouer un rôle important. Le 7 septembre dernier, j'ai signé avec Pierrick Massiot un partenariat de développement des activités de recherche duale, qui va tout à fait dans ce sens. Cette convention favorise le développement des PME. Elle permet le cofinancement et l'accompagnement, par la DGA et la région Bretagne, de projets innovants proposés par des industriels. L'expertise de la Bretagne en matière de cyberdéfense se distingue par son excellence ; elle doit le demeurer. Comme je l'avais annoncé en septembre 2012, deux cents emplois vont être créés au sein de DGA Maîtrise de l'Information, au profit du centre d'expertise technique pour la cyberdéfense du ministère de la défense. En 2017, nous aurons ainsi 400 experts de très haut niveau couvrant l'ensemble des domaines d'expertises technique de la cybersécurité : cryptologie, microélectronique, architecture d'équipements de sécurité et de systèmes, analyse de composants logiciels et matériels…

V)Conclusion

Mesdames et Messieurs,

Le cyberespace, dont nous ne faisons encore qu'effleurer les aspects les plus déstabilisants, est de toute évidence l'une des clés de notre défense et de notre souveraineté. Avec le Livre blanc de 2013, nous venons de poser la pierre d'angle de l'ambition nationale en matière de cyberdéfense. Pour présenter cette ambition, je tenais à m'exprimer devant vous, car je sais l'excellence que la Bretagne représente déjà dans ce domaine et, en même temps, tout le potentiel qui est encore le sien.

En ouvrant cette journée, je forme donc le vœu qu'elle soit fructueuse pour vous tous, et qu'à travers elle, vous fassiez vôtre l'ambition que je tenais à partager avec vous ce matin.