Le Livre blanc 2013 n'a pas fini de susciter des réflexions. Le président de la république s'exprimera devant l'IHEDN le 24 mai prochain. La pédagogie est toujours nécessaire pour exploiter un tel document d'autant que les critiques négatives persistent.

Je retiendrai l'article d'Isabelle Lasserre dans le Figaro du 17 mai Le Livre blanc ne tire pas les leçons du Mali qui me paraît bien résumer la situation déjà dans son titre. Le doute est présent. La réalité imprévisible de la guerre prochaine montrera si ce doute était justifié ou pas.

La question que je me poserai volontiers serait : qui devra porter la responsabilité devant l'échec éventuel d'une opération militaire ? Un gouvernement tomberait-il aujourd'hui suite à un tel échec ? Question bien sûr d'école mais à méditer : jusqu'à où faudrait-il remonter pour identifier les responsabilités ? Chaîne civile, chaine militaire, Livre blanc de 2008, Livre blanc de 2013… Et puis quel jugement, celui des urnes, celui de la justice suite à des plaintes de familles ayant perdu un proche au combat … intéressante problématique.

Revenons au Livre blanc de 2013 et à la prise en compte de la cyberdéfense dans le prolongement du précédent. Cela a été l'objet d'un colloque intéressant au Sénat ce jeudi 16 mai sur le thème « Quelles perspectives après le Livre blanc ? ».

Organisé par le Sénateur Jean-Louis Carrère, président de la commission des affaires étrangères, de la défense et des forces armées du Sénat et par le Sénateur Jean-Marie Bockel, ce colloque a été ouvert par Kader Arif, ministre délégué auprès du ministre de la défense. Je rappellerai que le sénateur Bockel a été le promoteur incessant de la prise en compte de la cyberdéfense.

Ce colloque a montré à mon sens un décollage vers une réelle prise en compte de la cyberdéfense bien que des faiblesses apparaissent mais ce domaine évolue si vite et il y a une telle remise en cause de notre vision stratégique.

Ce qu'il faut retenir est que la cyberdéfense est devenue une priorité nationale, qu'il existe une chaine de commandement cyber notamment pour faire face à des attaques de plus en plus sophistiquées venant souvent d'organisations non étatiques mais pas uniquement. Ce qui est apparu d'une manière très nouvelle dans cette journée ce sont les menaces clairement exprimées de l'espionnage et du sabotage, termes que l'on n'entendait plus, venant bien avant une cyberguerre.

Il faut donc augmenter les effectifs à l'image des autres alliés, former, sensibiliser. Le cyberdéfense militaire est renforcé ce qui semble une orientation nouvelle. Ainsi, un schéma directeur a été établi en juin 2012 pour aboutir en 2020. En juillet 2013, l'ANSSI et la chaine de commandement militaire seront colocalisées.

Il faut aussi protéger les systèmes d'information, être capable de riposter sans exclure l'action du ministère de la défense avec des capacités offensives étroitement associées au renseignement. Cependant une inquiétude réelle est apparue devant une sécurité assurée insuffisamment par les entreprises et aussi par les prestataires extérieurs à la défense.

C'est enfin un appel à une réserve dédiée au sein de la réserve opérationnelle. Elle sera

complétée par une réserve citoyenne organisée et développée pour la cyberdéfense, mobilisant en particulier les jeunes techniciens et informaticiens intéressés par les enjeux de sécurité.

Il a bien été évoqué l'identification de l'expertise pertinente pour répondre à ces menaces. Comme l'a rappelé FB Huyghe, ne faudrait-il pas s'intéresser à d'autres sciences que celles de l'informatique en se tournant vers celles celle du combat, de la stratégie en raison de leur finalité ? Cela conforte aussi mon sentiment : à force de penser la technique et donc le « comment ? », on oublie le « Pourquoi ? ». le cyber est un moyen et le véhicule d'idées qu'il faut savoir combattre au sein d'une stratégie générale où la réflexion doit primer sur l'outil.

La coopération européenne et internationale a été évoquée par Cornelia Rogall-Grothe, secrétaire d'état du ministère allemande de l'intérieur. Ce ministère constate cinq attaques par jour sur les institutions avec une courbe croissante. Le coût en est estimé en milliards d'euro ! 30M€ sont attribués pour les recherches en cybersécurité. Le besoin d'une souveraineté technologique européenne s'appuyant sur un marché intérieur conduit à une indépendance européenne, surtout pour avoir une plus grande confiance dans les produits fournis.

L'ambassadeur britannique Sir Peter Ricketts a rappelé quant à lui que l'économie numérique représentait 6% du PIB. 50 milliards de livres d'achats en ligne ont été effectués en 2012. 750 millions d'euros seront consacrés au cyber sur quatre ans en grande partie vers le GCHQ.

Mme Frédérick Douzet, titulaire de la chaire Castex de l'IHEDN sur la cyberstratégie, s'est penchée sur les Etats-Unis. Les cyberattaques sont considérées plus dangereuses que les attaques terroristes. Un quart des entreprises des Etats-Unis auraient été victimes d'attaques visant notamment à acquérir de l'information. 4,7 milliards de dollars sont consacrés au budget militaire « cyber », avec 900 personnes au « cybercommand » militaire dont l'effectif sera multiplié par cinq avec une vocation combattante et offensive.

Si je me réfère au Livre blanc, le cyberespace est désormais un champ de confrontation à part entière. Un scénario de guerre informatique constitue, pour la France et ses partenaires européens, une menace de première importance. La capacité de se protéger contre les attaques informatiques, de les détecter et d'en identifier les auteurs est devenue un des éléments de la souveraineté nationale. Et si on lit que la Chine est considérée comme une menace en raison de l'effort de modernisation de sa défense notamment dans ses capacités de cyberattaques, le champ des possibles est grand. En réponse à ces agressions, le Livre blanc précise même que, pour la France, *« Les opérations ciblées conduites par les forces spéciales et les frappes à distance, le cas échéant cybernétiques, pourraient devenir plus fréquentes »*.

Le constat de la menace rappelle cependant que l'Etat ne peut pas tout faire. Sa responsabilité vise avant tout à protéger les infrastructures critiques alors que la sécurité informatique doit être assurée par tous. la défense est effectivement l'affaire de tous.

Pour répondre à ces enjeux, l'État devrait donc fixer par un dispositif législatif et réglementaire approprié, les standards de sécurité à respecter à l'égard de la menace informatique. Les opérateurs devront donc prendre les mesures nécessaires pour détecter et traiter tout incident informatique touchant leurs systèmes sensibles. Tout ceci fera l'objet d'une doctrine nationale

pour répondre aux agressions informatiques.

Les enjeux sont donc réels. Une cyberstratégie est au cœur de notre défense nationale. Les armées devraient pouvoir y trouver légitimement toute leur place.