Conférence de l'Amiral Arnaud COUSTILLERE

« La transition numérique de la Défense nationale »

La prise de conscience de l'importance de la souveraineté numérique est récente, mais elle est maintenant réelle. A la notion de souveraineté numérique est liée celle d'autonomie stratégique. L'informatique ne se limite pas à ses extrémités visibles, soit environ 2%, l'essentiel ce sont les infrastructures qui représentent tout le reste : des investissements colossaux sans lesquelles on ne pourrait rien faire : les câbles grâce auxquels circulent les données et les data centers où sont stockées ces données. La souveraineté est battue en brèche, car les entreprises qui possèdent les infrastructures, les « GAFAM », possèdent également les données qui y transitent et y sont stockées. Le cloud, d'abord espace de stockage, mobilise en fait une puissance de calcul presque infinie, qui permet d'utiliser ces données au moyen de l'intelligence artificielle et de créer, grâce à elles, de la valeur. Mais les données que l'on confie, consciemment ou non, à des entreprises n'ont pas forcement lieu d'être commercialisées (données stratégiques, données concernant la santé des citoyens, la fiscalité…)

La prise de conscience de cette situation est de plus en plus forte. Le problème n'est plus un problème technique ou administratif, mais un problème politique, ainsi que le montre le conflit au sujet de Huawei entre la Chine et les États-Unis. La commercialisation à outrance des données a permis aux grandes entreprises américaines de s'implanter sur le marché mondial. Les Etats commencent à se saisir de ce problème. La France et l'Allemagne prônent ainsi la création d'un cloud européen pour sécuriser les données européennes et disposer de la puissance de calcul qu'offrirait un tel stockage.

Au ministère de la Défense, c'est le Livre Blanc de 2008 qui a marqué un tournant. Très influencé par le rapport remis en 2006 par le député Pierre Lasbordes « La sécurité des systèmes d'information : un enjeu majeur pour la France », il a donné lieu à la création de l'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information).

En 2011 a été créé un échelon, préfigurateur d'un nouveau commandement ; d'abord composé de trois personnes, il en comptait 3500 en 2017, dont un état-major de 80 personnes. Il devait s'attacher dès sa création à des propositions opérationnelles. D'abord placé auprès du sous-chef des opérations, ce commandement s'est dans un deuxième temps intégré dans le CPCO. Le principe du processus « cyber » est le suivant : s'intégrer dans les processus militaires et décliner les principes de combat pour les adapter au numérique, puisque désormais tous les processus doivent être adaptés aux problèmes numériques.

La difficulté majeure que connait le secteur numérique est celui des ressources humaines. Pour améliorer et faciliter les recrutements, un pôle d'excellence a été créé autour de Rennes. La Bretagne

a en effet une expérience ancienne en matière de télécommunications et des écoles spécialisées sont déjà implantées à proximité de Rennes. La Marine n'est pas loin, à Lorient et à Brest. Un pôle d'excellence a été créé en 2013 et un écosystème s'est développé, grâce auquel 10 % des start-up spécialisées se trouvent à Rennes. Un pôle de clients s'est également constitué pour créer une cellule de cyber-sécurité, France Cyber Maritime, destinée à la sécurité des armateurs et des ports civils. Il est porté par Brest-Métropole et présidé par le président du cluster maritime.

Il faut que les organismes ou les administrations restent maîtres de leur stratégie numérique : s'il n'y a pas une bonne maîtrise d'ouvrage lors d'une délégation, ce n'est plus une délégation mais un abandon à un prestataire. Pour cela, les ressources humaines sont l'élément essentiel. Dans le public comme dans le privé et dans tous les pays on assiste à une véritable guerre des talents. Or l'armée n'est pas la mieux placée car fonctions, statuts, salaires, conditions de recrutement et modes d'avancement sont multiples.