Participant à l'exportation du savoir-faire militaire français depuis de nombreuses années, le groupe Défense Conseil International entend compléter son offre avec la dimension cyberdéfense* qui est devenue une priorité nationale avec la parution du dernier Livre blanc. Theatrum Belli s'est entretenu avec le nouveau patron de DCI Jean-Michel Palagos. (propos recueillis par Stéphane Gaudin le 26 mai 2014).

TB : DCI souhaite développer le savoir-faire français en matière de cyberdéfense, quelles en sont les raisons ?

Jean-Michel Palagos : Pourquoi nous positionnons-nous dans le domaine de la cyberdéfense ? Pour bien comprendre, il faut revenir à la raison d'être de DCI : le transfert du savoir-faire des armées françaises, c'est-à-dire des armées proprement dites mais aussi la DGA et, plus largement, l'ensemble du ministère de la Défense. Notre ministre de la Défense, Jean-Yves Le Drian, a annoncé en février dernier un plan Cyber. En toute logique, dans la continuité de ce plan, nous nous positionnons sur ce qui est notre cœur de métier, à savoir le transfert de savoir-faire aux pays amis de la France.

C'est un sujet sensible. Je me souviens du discours prononcé par le ministre où il avait annoncé un doublement du nombre d'attaques cyber dont était victime le ministère en un an. Il y a donc un vrai sujet et une vraie demande. Les pays où nous sommes présents sont intéressés par le savoir-faire français. Pourquoi ? C'est dans la logique même de la position très singulière de la France, que l'on peut qualifier d'originale et d'indépendante. Cela s'est vu au cours de son histoire et je le ressens très régulièrement dans les pays amis où nous sommes présents : il y a à la fois une vraie reconnaissance de la position particulière de la France, un respect pour son savoir-faire et une envie de travailler avec elle pour bénéficier de ce savoir-faire.

TB : Quand vous parlez de « *pays amis de la France* », vous restez dans le cadre européen ?

JMP : A DCI, nous sommes principalement extra-européens. Nos pays historiques sont ceux du Golfe. Nous avons aussi une présence en Asie (Singapour, Malaisie) et au Brésil. Nous avons une présence qui a été plus importante dans le passé mais qui monte de nouveau en puissance en Amérique latine. Comme vous le constatez, nos pays historiques sont des pays qui sont en dehors de cette sphère traditionnelle que l'on pourrait qualifier de « sphère Otan » ou de « sphère européenne » ou de « sphère nord-américaine ». Ce sont des pays dans lesquels la France, dans son histoire et depuis longtemps, a entretenu des liens souvent très forts et encore très présents.

TB : Avec qui travaillez-vous ?

JMP : DCI travaille au transfert du savoir-faire des armées françaises (c'est le label « armée française ») et nous ne nous permettons pas de travailler en dehors de ce cadre. Cela veut dire que nous travaillons, dans le domaine de la cyber défense,très étroitement avec l'état-major des armées d'une part et avec la Délégation générale à l'armement (DGA) d'autre part. C'est dans ce cadre que nous proposons les formations cyber et jamais en dehors de ce cadre. Clairement, cela veut dire que nous n'avons pas la volonté de développer des offres qui

seraient, sinon contradictoires, du moins non cohérentes avec ce que fait, ce que peut faire ou ce que veut faire le ministère de la Défense.

TB : Quelles sont vos entreprises partenaires ?

JMP : Comme nous transférons un savoir-faire, en aucun cas nous nous occupons de la partie progicielle, logicielle ou équipements nécessaires dans le cadre de la cyberdéfense. Nous sommes donc dans une position très originale, à savoir que DCI est totalement indépendant de la totalité des industriels. Nous travaillons avec tous les industriels français qui interviennent dans la sphère défense mais nous n'avons de dépendance à l'égard d'aucun d'entre eux. Cela signifie que nous sommes en mesure de travailler avec tous les grands groupes qui investissent dans la cyberdéfense. Pour en citer deux et ce n'est pas exhaustif, je citerai Thales et DCNS. Mais d'autres interviennent aussi dans ce domaine, notamment des PME et des PMI innovantes.

Nous avons organisé au mois de février, une semaine après l'annonce du ministre, un séminaire du Cyber Defense Management Institute (CDMI). Plusieurs start-up y sont intervenues. Ce qui est important dans ce domaine, c'est la richesse de foisonnement intellectuel et créatif de ces entreprises, grâce à la complémentarité entre des petites entreprises et de très grands groupes qui ont une puissance dans leur savoir-faire. Nous avons aussi fait intervenir en introduction l'EMA et, au cours des travaux, la DGA a également été présente.

Encore une fois, nous ne faisons que de la formation. Il n'y a pas de transfert de technologie ni de transfert d'équipement**.** En fait, comme nous le faisons dans d'autres domaines (formation, conseil en équipement et du maintien en condition opérationnelle des équipements) nous participons très directement à la stratégie d'influence de notre pays à l'international.

TB : Vous assumez en quelque sorte un rôle de synergie entre les entreprises…

JMP : Oui et non. Oui, dans la mesure où notre indépendance nous permet de faire appel au meilleur de nos industriels, que ce soit des grands groupes ou des PME. Nous avons un rôle d'ouverture de porte et de synergie vis-à-vis de ces entreprises.

Non, puisque toutes ces entreprises ne sont pas dans une logique d'exclusivité avec nous. Elles peuvent très bien développer leur propre offre de prestations. Cela ne nous gêne pas du tout. Cela peut paraître curieux mais nous ne sommes pas dans une logique de concurrence avec ces entreprises. Pour nous l'important, c'est que cela soit la France qui gagne.

TB : Peut-on considérer que le fait que DCI choisisse telle ou telle entreprise permette à celle-ci, d'un point de vue marketing, d'obtenir un « label France » et « MinDef » lui procurant une forme de notoriété sur le marché…

JMP : Effectivement, cela sera plutôt sensible pour les PME. Les grands groupes n'ont pas besoin de nous pour ça. En tout cas, pour les PME-PMI, la réponse est oui. Ceci dit, je ne suis pas sûr qu'il y ait des cas où l'on travaille exclusivement avec l'un et l'autre. Il est probable que, dans la plupart des cas, la formation que nous allons dispenser, selon le besoin qui sera

exprimé par un pays ami, ce sera tel ou tel qui sera le mieux à même de répondre, en fonction de l'intensité demandée. La « cyber », vous le savez, est un domaine extrêmement vaste : de la simple sensibilisation de l'usager qui utilise un smartphone, au militaire qui a un équipement plus sophistiqué, en allant jusqu'à des spécialistes de protection contre les cyberattaques massives, le spectre de possibilité est gigantesque. Je pense même qu'on n'a pas encore mesuré toute l'ampleur du domaine de la cyberdéfense qui, au-delà d'une simple expression, tantôt employé comme « cyberdéfense » et tantôt comme « cybersécurité » a un domaine d'action très large. Dans certains pays, il s'agira simplement de sensibilisation et dans d'autres il faudra aller beaucoup plus loin.

TB : Pensez-vous que des majors puissent exercer une forme de pression par rapport à des PME-PMI dans le but d'imposer leur savoir-faire ?

JMP : C'est possible qu'il y ait un risque. Personnellement, je ne le pense pas parce-que les PME-PMI et les *start-up* sont dans des niches innovantes. Je vois surtout que tous les grands groupes, pratiquement tous ceux avec lesquels nous travaillons, ont une politique d'identification et de valorisation de *start-up* apportant un œil neuf, différent, très complémentaire de leur service de recherche et développement. Ils sont donc tous intéressés par ces PME-PMI. Je ne pense pas qu'ils aient l'intention de les écraser. Au mieux, il peut y avoir la tentation, à terme, de les intégrer dans un dispositif par des rachats. De toute façon, une *start-up* qui est rachetée par un grand groupe l'est parce qu'elle réussit. Le développement d'une *start-up* en un grand groupe est un succès. On a quelques exemples célèbres dans l'histoire. Mais son absorption par un grand groupe est aussi un succès car elle lui donne une capacité de développement considérable pour le domaine dans lequel elle intervient.

TB : Pouvons-nous avancer que DCI est un « fournisseur de souveraineté » pour des pays ayant constaté des failles…

JMP : « Fournisseur de souveraineté » est le bon terme puisque l'ampleur des menaces en matière de cyber est considérable. On cite des exemples d'attaques cyber qui ont paralysé des domaines entiers dans certains pays. Dans le domaine de la Défense, cela ne se dit pas trop car c'est un sujet trop sensible. Mais on le voit bien dans le domaine de la santé, ou d'autres secteurs. Il y a eu des attaques cyber qui ont considérablement amoindri les capacités dans certains pays durant une période plus ou moins longue. Donc il y a vraiment un sujet de souveraineté. Mais nous DCI, à quoi servons-nous ? Je n'ai aucun doute là-dessus. Nous avons été créés par le ministère de la Défense pour le transfert du savoir-faire des armées françaises. C'est notre génétique. Il est donc évident que nous devons accompagner les évolutions de ce ministère, les évolutions des armées et toujours en cohérence avec eux pour agir dans des domaines qui sont considérés comme prioritaires, que ce soit pour les propres moyens de la France mais aussi pour les pays amis. Je dis toujours « pays amis ». Pourquoi ? Parce que la France a des accords de Défense avec des alliés, avec des pays qui partagent, si ce n'est toutes nos valeurs, très souvent notre vision du monde. Il est important que DCI soit toujours en lien avec ça. Cela explique d'ailleurs la grande diversité des modes d'action de DCI et des domaines dans lesquels nous intervenons, qui ne se résument pas du tout à la formation et qui couvrent l'ensemble du spectre de ce que nous pourrions appeler une « offre capacitaire ».

Puisque, mise à part la production d'équipements, nous maîtrisons et transférons la totalité des savoir-faire des armées et de l'industrie de Défense, soit seuls, soit en partenariat.

TB : Et quels sont principaux concurrents dans ce domaine ? Je suppose les Américains en premier…

JMP : Si vous parlez du domaine cyber, c'est très difficile à dire. Tous les grands pays investissent aujourd'hui dans ce domaine : les américains (alors à chaque fois à l'échelle du budget du pays considéré bien évidemment) et les britanniques qui consacrent un investissement comparable à celui qu'on peut consacrer nous-mêmes (soit 1 milliard d'euros pour la France et 650 millions de livres pour la Grande-Bretagne). Il s'agit de grandes puissances qui ont un poids particulier dans le monde, qui ont une dissuasion, qui ont un système de défense performant et donc des intérêts à protéger. Tous ces grands pays investissent dans le domaine de la cyberdéfense.

Je ne raisonne pas en concurrence. Je pense que l'important, au niveau mondial, c'est qu'il y ait une offre de services, en l'occurrence pour nous simplement de formation. Chaque pays qui est intéressé par cette offre saura à qui s'adresser. L'avantage comparatif de la France est la grande qualité de ce que l'on fait, qui n'est jamais du *« low cost »,* mais de la « qualité France ». Ensuite, sur le plan stratégique, beaucoup de pays ne voient que des avantages à avoir comme partenaire un pays comme la France plutôt que d'autres.

TB : La dimension cyberdéfense permet-elle à DCI de proposer à des clients étrangers potentiels une offre de service plus « globale » en complément des systèmes d'arme ?

JMP : Nous raisonnons toujours en termes d'offre capacitaire. Cette expression est celle que j'emploie de plus en plus car elle résume ce que l'on fait : transférer une capacité à un pays. Cette capacité est celle qui permet de se défendre, de mettre en œuvre des équipements dont le pays dispose, de faire fonctionner de manière opérationnelle et interopérable les matériels. Effectivement, la cyber a un rôle à jouer dans ce domaine. Il n'est pas certain aujourd'hui que tout le monde ait bien compris le caractère global de l'ensemble de ces aspects. Souvent, c'est lié au système de décision qui peut être cloisonné : vous pouvez avoir un service qui va être chargé du *« training »* qui va vous parler de formation, un service qui est chargé du *« procurement »* et de la fourniture d'équipements qui va s'intéresser à l'accompagnement ou au maintien en condition opérationnelle des équipements. Mon objectif, c'est de faire comprendre ce caractère global que vous évoquez et dans lequel la cyber a sa place. Elle a sa place comme peut l'avoir le service de santé des armées avec le développement de son savoir-faire, le maintien en condition opérationnelle et la formation (formation de cadets, formation opérationnelle de spécialistes, l'ensemble des savoir-faire que maîtrise DCI dans son activité).

TB : votre secteur cyberdéfense comprend pour le moment combien de personnels ? Quelle sera sa montée en puissance dans un proche avenir ?

JMP : Nous disposons d'une dizaine de collaborateurs aujourd'hui et nous montons rapidement en puissance. Nous avons une première étape importante à la rentrée 2014 où nous allons travailler dans le cadre du pôle « cyber Bretagne ». Les étapes suivantes consisteront à

proposer de façon croissante aux pays amis nos formations cyber. Nous avons de bonnes perspectives, puisque notre premier séminaire a accueilli douze pays participants. Nous avons volontairement limité le nombre de participants parce que nous voulions rester dans un effectif maîtrisable en termes de formation et de présentation des savoirs.

Nous allons organiser un deuxième séminaire. Le premier séminaire a eu des effets assez originaux car il y eu des pays présents avec lesquels nous n'avions encore jamais travaillé comme le Mexique et plusieurs pays de l'Europe de l'Est… Nous avons donc pu confirmer que cette approche de la cyberdéfense suscite un intérêt très important. Notre développement ira toujours dans le cadre de ce qui sera possible, crédible et souhaité par le ministère de la Défense. Nous ne serons jamais ni en prédation ni en excès de transfert si ce n'est pas utile ou si ce n'est pas jugé pertinent. Nous ferons toujours preuve d'une grande prudence dans le transfert des savoir-faire dans ce domaine.

* **La cybersécurité est l'état final des systèmes et des actifs d'une entité après que les mesures de protection et de défense aient été mises en œuvre. Les activités cyber couvrent : l'Anticipation (veille/R&D), la cyberprotection (plus connu jusqu'ici sous le vocable SSI) et la cyberdéfense active. Cette dernière, généralement mise en œuvre par une entité régalienne ou un « OIV » (Opérateur d'Importance Vitale), reprend les fonctions opérationnelles principales en usage dans les armées : surveillance/situation, planification et opérations. La cyberprotection couvre le management de la sécurité, la sécurité des infrastructures gérées par un opérateur et les « facilities ».**

Lire aussi : Le magazine des ingénieurs de l'armement sur la cybersécurité (mars 2014)