Taking part since years in the exportation of French military savoir-faire, the *Défense Conseil International* (DCI) group wants to complete its offer through the cyber-defense dimension, which has become a national priority with the publishing of the latest *Livre blanc* [1]. Theatrum Belli interviewed DCI's new CEO, Jean-Michel PALAGOS. *(Recorded on the 26th of May, 2014 by Stéphane Gaudin).*

TB : Why (for what reasons) does DCI intend to develop the French know-how in cyber-defense?

Jean-Michel Palagos : Why do we position ourselves on the field of cyber-defense? To understand fully, one may focus on DCI's raison d'être: sharing the savoir-faire of French armed forces, i.e. of forces strictly speaking, plus the DGA [2] and, more widely, the entire ministry of defense. Our defense minister, Jean-Yves Le Drian, announced last February a cyber-defense plan. Logically, in the aftermath of this plan, we position ourselves on what is our core business, namely savoir-faire sharing with France's allies.

It's a sensitive topic. I can remember the speech pronounced by the minister, when he told that the number of cyber-attacks perpetrated against the ministry had doubled within a year. There is therefore a real issue and a real demand. The French know-how appeals to the countries where we are present. Why? It results from the particular position of France, which may be described as original and independent. It is visible through its history and I can feel it regularly in allied countries where we are present: there is, at the same time, a genuine acknowledgement of the particular position of France, a respect for its savoir-faire and a desire to work with it in order to benefit from this savoir-faire.

TB : When you are talking about "France's allies", do you stay in a European framework?

JMP : At DCI we work mostly on an extra-European level. Our historical countries are in the Gulf. We also have a footprint in Asia (Singapore, Malaysia) and in Brazil. We used to be more present in Latin America in the past, but now it is increasing there again. As you can see, our historical countries are out of this traditional sphere we could call the "NATO sphere", the "European sphere" or the "North-American sphere". These are countries where France, throughout its history and since a while, has sustained links that are often very strong and still very present.

TB : With whom do you work?

JMP : DCI works on the transfer of the French armies' know-how (it's the "French army" label) and we don't venture out of this framework. In the field of cyber-defense, this means that we work closely with the joint chiefs of staff on one side and the Direction générale de l'armement (DGA) on the other. We propose our cyber trainings in this frame, and this frame only. Clearly it means that we don't wish to develop any offer that would be, if not contradictory, at least not

coherent with what the ministry of defense is doing, can do or intends to do.

TB : Who are your partners in business?

JMP : Since we share savoir-faire, we never deal with the software aspect and the equipment necessary to cyber-defense. We are therefore in a very particular position, as DCI is fully independent of any industrial stakeholder. We collaborate with all the French industrialists who take part in the defense sphere but we have no dependency at all on any of them. It means that we are able to work with all the big companies which invest in cyber-defense. The list isn't exhaustive but I would cite two of them: Thales and DCNS. However, many others participate in this field, namely some innovating SMEs and SMIs.

One week after the minister's speech, we organized last February a symposium of the Cyber Defense Management Institute (CDMI). Several start-ups intervened there. In this field, the important thing is the wealth of intellectual and creative profusion of these businesses, thanks to a coalition between smaller companies and some very big groups which have a power in their savoir-faire. As an introduction, we had the French Joint Chiefs of Staff intervened, and during the panels the DGA was also present.

Once again, we only supply the training. There is no technology or equipment sharing whatsoever. Indeed, as we act in other fields (training, consulting in equipment and maintenance in operational conditions for equipment), we directly participate in the influence strategy of our country on the international scale.

TB : Somehow you assume a role of synergy between businesses…

JMP : Yes and no. Yes, insofar as our independence enables us to call on our best industrialists, be it a big group or an SME. We play a role of door-openers and of synergy initiators towards these businesses.

No, considering that all these businesses do not follow a logic of exclusivity towards us. They are free to develop their own package of services. It does not bother us at all. It might look strange, but we do not follow any competitive logic vis-à-vis these companies. To us, what matters is that in the end France prevails.

TB : Can we consider on a marketing level that when DCI choses this or that company, this allows the latter to get a "France" or "MinDef" [3] label, which would make their notoriety on the market increase…

JMP : Actually, it will be more perceptible for SMEs. The big groups do not need us for this. Anyway, the answer is yes for SMEs and SMIs. Then again I am not sure there is a single company we exclusively collaborate with. It is likely that, in most cases, the training may be provided by the most qualified collaborator available, according to the demand expressed by an allied country and the required intensity. You know that cyber-defense is an extremely large field: from the basic awareness of a smartphone user, the soldier using a more sophisticated

gear, to specialists in charge with protection from massive cyber-attacks, the range of possibilities is immense. I even think we haven't estimated fully yet the vastness of the cyber-defense field, which covers a very large area for action, beyond a simple expression referring either to cyber-defense or cyber-security. In some countries, a simple awareness building will be enough and in others one must go much further.

TB : Do you think that major companies might lobby some SMEs and SMIs in order to impose their savoir-faire?

JMP : There might be a risk. Personally, I don't think so because SMEs, SMIs and start-ups evolve in an innovating technological niche. I observe that all the major groups, basically all of those we work with, have a policy of identification and of promotion towards the start-up which sees things in a new different perspective, complementary to their research and development department. They are all interested in working with these SMEs and SMIs. I don't think they intend to crunch them. At best, there might be a temptation, eventually, to integrate them into a system through buyouts. Anyhow a start-up is purchased by a big group because it is successful. And the mutation of a start-up into a big group is a success. There are some famous examples in history. Moreover the incorporation of a start-up into a group is a success also because this brings a considerable capacity for development in the start-up's activity field.

TB : May we put forward that DCI is a kind of sovereignty supplier for countries which noticed loopholes…

JMP : "Sovereignty supplier" is the exact word, because the scope of threats in cyber-defense is huge. There are many examples of cyber-attacks that paralyzed entire sectors in some countries. It is not often evoked in relation to the defense sphere, the topic being too sensitive. But it is noticeable concerning healthcare or other fields. Cyber-attacks occurred in some countries where they considerably weakened their capacities over more or less extended periods. There is indeed an issue of sovereignty. And what is DCI's role? I have no doubt whatsoever about it. We were created by the ministry of defense to promote and share the know-how of French armed forces. This is our genetics. It is clear that we shall follow the evolutions of this ministry, the evolutions of the armed forces, always in accordance with them to intervene in fields regarded as priority, be it for France's own resources or allied countries'. I always say "allied countries". Why? Because France has defense agreements with allied nations, countries that share, if not all our values, but very often our worldview. It is important for DCI to always be connected to this. This explains, by the way, the large diversity of DCI's courses of action and intervention areas, which are not limited to training and include the whole spectrum of what could be called a "capacity offer". Since, the equipment production apart, we master and share all the forces' and defense industry's know-how, either by ourselves or within partnerships.

TB : And who are your major rivals in this field? I assume the Americans are in the lead…

JMP : Hard to say if you are talking about the cyber sector. All the big countries now invest in this sector: the Americans (always on a scale in accordance with the individual country's budget of course) and the Brits who allocate an investment similar to France's (i.e. 1 billion euro for France and 650 million pound for Great Britain). They are great powers which have a particular influence worldwide, a deterrent, an efficient defense system, and therefore they have interests to protect. All of these big countries invest in cyber-defense.

I don't think in terms of competition. What matters globally is to have an offer of services, which in our case is simply training. Every country interested by this offer will know whom to ask. The comparative edge of France is the great quality of what we do, which is never low cost but "Made in France quality". Then, on a strategic level, many countries only see advantages to have a country like France rather than others as a partner.

TB : Does cyber-defense dimension enable DCI to propose a more "global" service offer as a complement to armament systems to potential foreign customers?

JMP : We always think in terms of capacity offer. I use this expression more and more often because it sums up what we do: transmitting a capacity to a country. This capacity enables to defend oneself; to make use of equipment the country has at its disposal; to make the tools work in an operative and interoperable way. Indeed, cyber has got a role to play in this field. It is not so sure today that everybody has well acknowledged the global nature of all these aspects. It is often related to a compartmentalized decision-making system: you can have a unit responsible for "training" who will talk about training; another unit responsible for procurement and gear supplying who will be interested in coaching and maintaining equipment in operational conditions. I aim at highlighting this global aspect you mention, which cyber-defense is a part of. It plays a role in it as do the defense health service with the development of its own savoir-faire, the maintenance in operational conditions and training (training for cadets, operational training for specialists, all the know-how mastered by DCI).

TB : How many people work for your cyber-defense sector today? How will this evolve in the short term?

JMP : Today we have a staff of about ten or so and our activity is increasing fast. Fall 2014, we will intervene within the framework of the "cyber-Bretagne" [4] pole, which is a very important first step for us. The steps coming next involve proposing more and more our cyber trainings to allied countries. We have good prospects because 12 countries took part in our very first seminar. The number of participants was limited on purpose; our intention was to maintain a reasonable headcount to provide better quality for the training and the diffusion of knowledge.

We will organize another seminar. The first one had rather original effects because countries like Mexico or from Eastern Europe were present, with whom we had never worked before... We had confirmation, therefore, that this approach of cyber-defense attracts considerable interest. We will always develop in the limits of what is possible, credible and in accordance with the ministry of defense. We will never be either predators or over-sharers, if it is not useful or not considered relevant. We will always stay highly cautious about sharing know-how in this

sector.

Interviewer : Stéphane GAUDIN

Interviewee : Jean-Michel PALAGOS

Recorded : May 26th, 2014

Translation into English for Theatrum Belli : Robert ENGELMANN

[1] It refers to the reorganization plan of French armed forces (2014-2019)

[2] Approximate translation : General Directorate of Armament

[3] Short for “Ministère de la Défense”

[4] A pole of excellence dedicated to cyber-defense soon implemented in Brittany