The new CYBER weapon is being built within the US Army...

military-Earth thinking notebook

le Lieutenant-colonel Hyacinthe de LAVAISSIÈRE

Published on 18/10/2018

Sciences & technologies

The French Ministry of Defence has been making a very significant effort in recent years to improve our computerized combat capabilities, in liaison with other government departments. This effort is particularly taken into account and relayed by the French Army in the framework of its future "In Touch! model". It therefore seemed interesting to inform the readers of the Cahiers on the evolution of the US Army in this field, thanks to a summary article written by one of our liaison officers in the United States.

At the Augusta TechNet 2015 conference, Major General Stephen Fogarty, commander of the US Army CyberCenter of Excellence at Fort Gordon, noted that the foundation stone of the new cyber weapon had been laid, but that the next step was to bring together all those involved in the effort to provide a fully integrated tool for operations. Indeed, the foundations for the cyberweapon, in the human resources sense, are now in place and recruitment in all categories has begun.

Far from phagocyting signals and intelligence, the cyberweapon must ensure the US Army'slong-term capacity to arm 41 qualified and trained cyber teams, whose combatants will be managed individually. In contrast to the search for mass effect, this force will be counted to ensure a high level of expertise and unity of action in cyberspace.

The Army Cyber Force built **on the joint model**

Since 2011 and on the orders of US CYBERCOM, the US Army is contributing to the Joint Cyber Mission Force with a volume of approximately 6,200 combatants.

The Joint Command has defined the missions, structures, roles and tasks. As soon as they were qualified and trained, the elements of the force were engaged in operations without waiting for the human resource maneuver. Thus, the creation of a cyber weapon within

the US Armywas not imposed, but rather responded to a requirement for coherent career paths for the future.

While for land operations the basic unit of the US Army is the Combat Team Brigade, for cyber operations the basic cell is the team. Regardless of the army to which the men who arm these teams belong, they must be qualified according to the criteria of one of the 14 joint workroles. These 14 roles make it possible to build the different teams that make up the CMF.

The USArmy is contributing to the joint effort by building 41 cyber teams out of the 133 planned by US CYBERCOM. Currently in the ramp-up phase, the Army CyberWorkforce is already 50% operational as it is actually being built since 2011 from existing weapons and specialties.

The new Cyber Weapon for a fine management of the resource

Overall, most of the profiles sought exist in the signals, intelligence and artillery weapons. On the other hand, each selected soldier must follow a training cycle that requires up to six months of adaptation courses before joining a team. In fact, the 41 teams represent 1,899 combatants, 65% of whom come from the intelligence service, 34% from signals and 1% from artillery. This intelligence tropism is even more flagrant in the case of the National Teams or Combat Teams where the ratio exceeds 87%. On the other hand, 77% of the Cyber Protection Te ams are made up of transmitters and only 35% of intelligence personnel, which reflects the defensive nature of their mission. However, they still have a Red Squad specialised in the study of the opponent's modes of action.

In this force, the presence of civilians in specialties 0132 (intelligence) and 2210 (information systems), which account for 16% of the total volume, should be noted. These civilians, more than half of whom are former military personnel, are very present in Army structures and often constitute crucial expertise. Finally, the presence in the teams of 104 people from intelligence agencies illustrates the support provided by those agencies and the strike force they represent as a complement to this military cyber force. Thus, while the figure of 6,200 men announced for the Joint Cyber Force already seems a little underestimated, it would be necessary to add to it the manpower of the National Security Agency and that of other agencies to evaluate the reality of the American cyber force.

Considering the investment in training, the US Armywanted to protect this resource and build complete career paths by creating a new weapon, the Cyber Branch 17. Recruitment is being done both through reclassification and direct entries such as the 32 second lieutenants who arrived this year. With this initial stage almost complete, the next phase will be to integrate the electronic warfare personnel, previously managed by the artillery. This project is therefore far from being completed, especially as the development of professional paths has only just begun. Eventually, the convergence of signals - electronic warfare - intelligence - fire could lead to structural changes with an impact on the conduct of operations.

Thus, if the new cyber weapon is on the way to reaching its first thousand combatants, its rise in power should last until 2017. Almost paradoxically, nearly 50% of the 41 cyber teams, both offensive and defensive, are already operational and at work on the orders of US CYBERCOM.

Lieutenant-Colonel Hyacinthe de LAVAISSIÈRE belongs to the US Army Land Liaison Detachment, and serves as liaison officer to the Cyber Center of Excellence at Fort Gordon.

Title :	le Lieutenant-colonel Hyacinthe de LAVAISSIÈRE
Author (s) :	le Lieutenant-colonel Hyacinthe de LAVAISSIÈRE
Release date	08/10/2018