The conquest of human resources in cyber defence

BRENNUS 4.0

le commandant Jean-François Caverne, officier stagiaire de l'EMSST (cycle académique 2018-2019)

Published on 25/03/2020

Sciences & technologies

In September 2017, General Olivier Bonnet de Paillerets became the first cyber defence commander in French history. He succeeds Vice-Admiral Arnaud Coustillière, General Cyber Officer. The creation of the French Cyber Command (COMCYBER - attached to the Armed Forces Staff) and this new appointment are the logical continuation of the wish of theThe creation of the French Cyber Command (COMCYBER - attached to the Army Staff) and this new appointment are the logical continuation of the wish of former Defence Minister Jean-Yves Le Drian to see the emergence of a fourth autonomous army, alongside the Army, Navy and Air Force. While this fourth army is still a pipe dream, the creation of this command, comprising a reduced central headquarters and a few units, is the first stone that will underpin the new French cybernetic component of the Ministry of the Armed Forces (MINARM).

This strategic choice, made by France over the last decade, should not, however, cause us to forget the lead taken by other powers (France, Germany, Italy, the United Kingdom, the United States and the United Kingdom).This strategic choice, made by France over the last decade, must not, however, overshadow the lead taken by other powers (United States, Russia, China) in this field and the need to have a scarce qualified human resource to propose a coherent, solid and above all credible model in the long term. More than in any other operational area, cyber defence is above all a matter of acquiring high-level technical skills which must be maintained and updated over time.

While the cyber defence component is nowadays considered to be an essential vector for the success of military operations and national sovereignty, the fact remains that this nascent component must be consolidated and win the battle for human resources. One promising avenue would be to federate initiatives and develop a comprehensive military cyber defence sector to increase the attractiveness and visibility of a rapidly expanding field in search of rare and much sought-after resources.

To understand how to meet this challenge of robustness and efficiency, we must first consider the young model chosen by France. Next, it must be understood that the resource must not be reduced to the technical dimension alone, but rely on the involvement of all staff for the benefit of the strategic project. Finally, the scarcity and volatility of resources leads us to look at capitalizing on different initiatives to develop a strategic sector.

A coherent model to be consolidated

After the "cyber defence pact [1]" which aimed to put MINARM in battle order to adapt it to the challenge of cybernetics, the advent of the "cyber defence pact" was followed by the "Cyber Defence Pact" [2].The advent of COMCYBER [2] is intended to federate and boost all cyber defence forces after a decade of effort in this field [3]. This component is based on a timeless principle: the security of systems depends on the people who implement it. Any actor can access the technology with the necessary funding. What makes and will make the difference is the quality of the human resources and the model that integrates them.

The creation of a fourth cybernetic army, as called for by former Defence Minister Jean-Yves Le Drian, would be an ideal response for manoeuvring on the cybernetic battlefield. This model of army would be atypical and observed by all. It would open an ambitious path different from the choices of other cybernetic powers, such as the United States and China.

But this creation could lead to a loss of coherence by siphoning off the pool of specialists from the different armies and create loopholes in an area that, on the contrary, must be brought together and shared since it is omnipresent in our weapon systems. By relying on a joint command, COMCYBER seems to be "the best way", as Admiral Coustillière points out. Moreover, it offers a centralization of capabilities to allow a thorough reading of the evolution of the threat, to ensure control of resources and to homogenize methods over the totality of possible engagements. COMCYBER covers and distinguishes between offensive, defensive and intelligence missions through separate units to effectively cover the broad spectrum of the cyber threat.

Above all, COMCYBER's human resources must enable it to cover a wide spectrum of trades and activities. Without "digital fighters" in quality and quantity, COMCYBER would be an empty shell. Therefore, it needs highly qualified personnel in sufficient numbers, as formalized in axis 3 [4] of the Cyber Defence Pact [5]. The 2019-2024 military programming law therefore doubles its strength to 2,600 by the end of 2019 (plus 4,400 reservists) with the support of 600 experts from the Directorate General of Armaments.

The challenge of change

Beyond a collective awareness of the importance of cyber defence, the coherence of the military cyber component also requires a change of mentality. " Security has long been considered an unavoidable and costly necessity linked to risks and uses [6] . 6] Threats have evolved and today's cyber defence is no longer yesterday's Information Systems Security (ISS). The likelihood of certain threats, once unthinkable, is now a reality. In order to eliminate the risk, it is necessary to continue to implement a proactive approach to change mentalities, in order to reinforce the involvement of everyone for the benefit of the strategic project.

The current access to various cybernetic technologies represents a misleading asset for our executives and decision-makers. "If we are satisfied with the most widespread opinion, technology would be the decisive asset in the fight [7] ". 7] This simplistic, yet popular, shortcut could lead people to believe that the digital tools in our possession and the industrial support in this field are sufficient, making us untouchable and powerful. The real asset in cyber defence is the timeless principle of specialized human resources. Without competent and numerous human capital, our units and tools will not reach their full potential.

Secondly, like society, ideological differences may exist between "pro-cyber" and "anti-cyber". They are a source of weakness. It is a fact: the new cybernetic uses are helping to change the way the armed forces operate, the conditions and framework of engagement, but also the daily life of the military. The sophistication of the tools and the feeling of loss of control can be worrying. An ideological trap can be created: "The test of fire is often cruel for new ideas. The first use of tanks by the British in September 1916 and the French on 16 April 1917 (76 out of 121 machines destroyed) was disastrous. The first major Allied airborne operation, in 1943 in Sicily, was a fiasco [8]" .

The cyber sector is characterized by a general dynamism. Technologies and resources are constantly evolving. New skills are confronted with new expectations. The very recent digital fighters are largely from generations Y and Z, who cannot live without constantly looking for signs of recognition. These "connected generations" are the subject of studies and new managerial approaches in the private sector. Their need for attention and a search for meaning in their work are essential to gain their support. The driving force behind their commitment is therefore special attention, despite, in cyber defence, the low visibility of their field of action.

If this internal recognition is useful for cyber defence resources, it becomes a determining factor in attracting and retaining future digital fighters.

The conquest of resources

The real battleground for the cyber defence component is the recruitment of high-level technical skills. All private and public actors today face difficulties in attracting personnel in a field with strong competition in the labour market. A study based on the return of 19,000 IT security specialists estimates that 1.8 million qualified cybersecurity resources are expected to be in short supply worldwide by 2022 [9]. A forecast revised upwards by 20% compared to 2015. This shortage will result in a hiring deficit and a decline in the quality of the staff recruited. However, cybernetic operational capabilities are directly dependent on specialized human resources. The scarcity of resources therefore makes it necessary to increase the attractiveness of the cyber defence sector by providing greater clarity on the field and visibility on the career paths on offer.

At the global level, as in France, profiles specialising in cybersecurity are therefore highly coveted. " Only 25% of recruitment needs in the sector were covered in 2015 [10]" .

"The shortage will continue for at least 5 years [11]". It is and will be difficult to attract and retain skills. The job market offers are plentiful and offer remuneration levels that are difficult to match. "A level 1 support technician in a Security Operations Center (SOC) can earn around 40,000 euros per year, a level 3 analyst can claim 65,000 euros, while the SOC manager will have no trouble finding a job at around 80,000 euros [12] ". Large groups such as EADS, Thales, Orange, Sogeti, Alcatel-Lucent, Capgemini, etc. are intensively recruiting coveted resources. To be attractive, an adapted index grid or a technicality bonus are possible solutions. The Gendarmerie and the French Ministry of Finance are therefore promoting these rare profiles.

This tension over highly coveted profiles makes it necessary to find other levers of attractiveness. The winning challenge for the armed forces would be to create a young and diversified pool of young people familiar with the issues and missions of the Ministry of the Armed Forces. In order to capture a scarce resource on the job market, the youngest must be attracted and retained before they enter the job market. Recruiting a young resource makes it easy to acculturate them to the military field and, above all, to retain them as early as possible by offering candidates an esprit de corps and status that will make them want to make a long-term commitment. The idea remains to motivate and involve potential recruits by offering them support and opportunities for development based on merit. The latter will enable them to take up personal and professional challenges during their career and to maintain their membership. The conquest of the workforce will be made with young people who are aware of the military specificity, who have been offered clear perspectives and marks of recognition thanks to which they will feel involved and valued.

While the lack of candidates is a major cause of recruitment difficulties, "the main problem is not the insufficient number of places or training (initial or continuing), but more generally the attractiveness ofthetraining and the sector [13] ". 13] This problem affects all recruiters. Candidates are high school and university students seeking visibility and recognition. The right profiles should therefore be oriented towards the cybersecurity training courses of the Ministry of the Armed Forces that correspond to them, in order to meet the professional needs and expectations of the military institution. This is a decisive point in achieving the desired end state.

Finally, a valorisation of the cyber defence professions is necessary for recruitment, but also for retention.

THE CHALLENGE OF BUILDING LOYALTY

While young and diversified recruitment is an essential prerequisite for obtaining a coherent HR model over time, it is imperative to ensure the preservation of this rare resource. Turnover is considerable in this area. Loyalty is at the heart of the preoccupations to make the investment made on these resources profitable. Their natural volatility is such that it encourages the identification of bold initiatives. The federation of these initiatives will structure and enable the development of a strategic sector.

In order to maintain their pool of specialists, the armed forces are perfecting training courses focused on the different profiles sought (non-commissioned officers, officers and defence civilians). These training schemes, which are based on a "win-win" investment, are a considerable help in combating the attrition rate in this field. The awarding of qualifications recognised in the national directory of professional certifications, with a guarantee of employment upon leaving school, is a decisive lever for making the cyber pool of skills more secure. The example of the Saint-Cyr-l'École military high school is an interesting one. Launched at the beginning of the 2017 academic year, a BTS in cyber defence, unique in France, offers professional opportunities within MINARM. On 31 August 2015, the Saint-Cyr Coëtquidan military academies launched the specialized master's degree in "Cyber Defence Operations and Crisis Management". The Army has developed the awarding of scholarships to enable cybersecurity students to carry out their studies in a field they are passionate about, with a first professional contract within the Army.

The creation of the Cyber Excellence Centre in Brittany (PEC), enhanced by various partnerships between companies, MINARM units and higher education establishments, is a decisive initiative to facilitate entry into the field and encourage long-term vocations. Regional attractiveness is a promising choice, following the example of Silicon Valley in the United States . The development of the Brittany Cluster will support the construction of qualifying and coherent career paths combining the satisfaction of MINARM's skill requirements and the mobility of civil and military agents [14]. Moreover, the partnerships signed in the framework of the CEP could offer opportunities for the secondment of military personnel to reference companies established in this centre. As the Gendarmerie does with major accounts, this would make it possible to offer experiences and feedback that would be enriching for all parties.

Within MINARM, there is a seam that is still under-exploited: the Cyber Defence Citizen and Operational Reserve contributes to developing the diversity of courses in cyber defence. This lever allows the retention of resources that are difficult to access, or even untouchable, through direct military recruitment: consultants, employees, researchers, etc. Its aim is to bring visions, experience and skills that complement the resources already acquired, while allowing them to spread their influence. It is already a success because it will involve more than 4,400 people in 2019. But it is still a challenge because we need to be able to retain this staff over the long term. The attractiveness of this channel needs to be maintained in order to attract people who are passionate about the Internet and aware of national issues.

More than in any other operational area, winning staff must be the primary objective guiding cyber defence. In order to overcome cyclical difficulties and offer a balanced model that meets France's needs over the coming decades, we must capitalize on promising initiatives in recruitment, training, loyalty and internal recognition. The success of future cybernetic operations could depend on the ability to meet this challenge in the future.

1] See Annex.

2] Id .

3] Id .

4] "Strengthening human resources dedicated to cyber defence and building associated career paths".

5] Ibid .

[6] Sopra Steria publication.

[7] JOZEFOWICZ, Henri, Technologie : l'atout trompeur, Défense et technologies, Cahiers Pensée mili-terre, issue 48 - 3ième trimestre 2017, Centre de Doctrine et d'Enseignement du Commandement, page 3.

8] Des électrons et des hommes, Cahier de la recherche doctrinale, Centre de doctrine d'Emploi des Forces, 2005, page 11.

9] International Information Systems Security Certification Consortium (ISC2), "Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher," https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage, accessed 08 September 2018.

10] ANSSI estimate, Les Echos.fr, "Cybersecurity: desperately seeking candidates", January 2016.

11] David Majorel, quoted by Philippe Richard, "La France manque d'experts en sécurité informatique", section Informatique et Numérique des Techniques de l'ingénieur, https://www.techniques-ingenieur.fr/actualite/articles/france-experts-securite-informatique-39712/, consulted on 08/09/2018.

12] Ibid .

13] Study "Training and skills in France on cybersecurity" carried out by the firm EY on behalf of the Observatoire Paritaire de l'Informatique, de l'Ingénierie, des Etudes et du Conseil (OPIIEC), RAPPORT D'ETUDE May 2017, page 70.

14] Axis 3 of the Cyber Defence Pact.

Title :	le commandant Jean-François Caverne, officier stagiaire de l'EMSST (cycle académique 2018-2019)
Author (s) :	le commandant Jean-François Caverne, officier stagiaire de l'EMSST (cycle académique 2018-2019)
Release date	17/03/2020

FIND OUT MORE