Towards a new cyber army? Breton?

military-Earth thinking notebook

le Chef de bataillon Arnaud BALLER

Published on 25/05/2018

Sciences & technologies

Since the publication of the LBDSN 2013 making cyber defence a national priority, a Breton dynamic has emerged, suggesting that a fourth army could be created. However, although many factors legitimize this development in Brittany, it is part of a more global approach aimed at a transversal deployment of cyber capabilities within the Ministry.

At the beginning of December 2014, the American company Sony Pictures Entertainment announces that the equivalent of more than 3,000 digital data DVDs have been pirated. This computer attack, one of the largest ever suffered by an American company, highlights the fragility of the cyber world, a constantly evolving field.

"Just imagine a firing computer that breaks down when responding to a raid by opposing aircraft, or the propulsion of a ship that no longer responds. Our armed forces have to deal with this new situation. They must - you must take ownership of this new space of conflictuality [cyberspace], both to defend yourselves, but also to operate in it in support of our operations". These words of the French Minister of Defence, when he came to the DEFNET exercise in October 2014, a few weeks before the "Sony affair", clearly show the will and the need for the Ministry of Defence to face these new threats. The LBDSN[1] of 2013 had indeed endorsed the idea that cyberspace had become, after land, air, sea and space, a fifth field of confrontation in its own right, and cyber defence[2] a national priority. 2] Since then, a desire has emerged to equip armies with both offensive and defensive capabilities. In particular, there has been a desire, which has received a lot of media attention but is highly controversial due to the Breton origins of the Minister of Defence, to make Brittany a cyber defence centre of excellence.

It is therefore interesting to identify and understand the reasons that really motivated the deployment of such capabilities in the Great West. How is this desire expressed and what does the future hold for this centre of excellence? More generally, in a constrained economic context, is the creation of a "fourth cyber army" anchored in Brittany envisaged

and/or conceivable?

Many factors justify and legitimize a cyber development in Brittany that is part of a more global approach aiming at a transversal deployment of cyber capabilities within the Ministry of Defence.

A legitimate choice ...

- A legacy of General de Gaulle...

At the end of the 1950s, Charles de Gaulle, President of the Republic, wanted to give economic impetus to France and, through the Commissariat Général du Plan, oriented Brittany towards the field of electronics and telecommunications. The inauguration of the CNET[3] in Lannion in 1959 thus marked the beginning of the Breton appropriation of know-how in this field. This political will, giving the region an electronic vocation, as Marie Carpenter evokes in her work "The battle of telecoms - Towards a digital France". (2011), initially based on land use planning, has allowed a real Breton positioning in a sector with a future. Information technology having taken on more importance in the 1980s, with an increasingly sought-after networking, digital skills, particularly in relation toThe IT sector took on greater importance in the 1980s, with an ever-increasing demand for networking, and digital skills, particularly in the area of information systems security, emerged in Brittany, giving the region a specific digital character.

- ... made this region a catalyst for digital development ...

This legacy has enabled the region to weave a dynamic local network in this highly technical field by relying on a dense industrial fabric, active research, but also and above all a wide range of training opportunities. A direct consequence was the deployment in 2005 of the "Images and Networks" competitiveness cluster, which provides Brittany with a strong R&D capacity. In addition to major industrial groups such as Orange, Capgemini and Technicolor (formerly Thomson), which have set up their technical centres in Brittany, the region has an incubator for SMEs with activities focused on digital technology and its security. Since 2009, when the RAPID [4] scheme was set up, 30% of the funds relating to digital technology and its security have been granted to Breton SMEs. B-com, one of the eight French technological research institutes, chose Rennes as a home base for developing and selling skills in the digital field at the beginning of 2012. This complementarity between research and the industrial world is complemented by quality teaching through numerous schools such as Supélec and Télécom Bretagne, which since 2002 have been co-delivering one of the first training courses in computer security. The many partnerships established between these schools and the industrial world make it possible to create the necessary link to this local network.

- ... conducive to the development of a military cyber capability in Brittany

At the beginning of 2012, the establishment of a military cyber capability in this particularly attractive region has been studied by the Ministry of Defence and the Armed Forces Staff. This development had become necessary to face the new digital threats mentioned in the LBDSN of 2008, but which were only really taken into account after the end of the war.This development had become necessary to deal with the new digital threats mentioned in the 2008 LBDSN, but was only really taken into account after the

major cyber attacks of Stuxnet (2010) and Flame (2012), which respectively slowed down Iran's uranium enrichment programme and infected more than 1.000 computers for counter-intelligence purposes. The aim was then to take advantage of this local synergy while drawing on a pool of existing military capabilities in order to develop national competence, both for day-to-day operations and for deployment in external operations. DGA MI[5], present in the Rennes region since 1968, provides the Ministry with high-level technical expertise in research, but also in the development of tools. Moreover, the numerous defence training organisations (ESCC, EN and ETRS[6]) could provide the local training component necessary for the deployment of any new capability. Finally, the Coëtquidan camp had all the facilities to become the ideal training space for the operational preparation of new units.

This favourable environment, whether military or civilian, enabled the Ministry to be responsive in initiating a local dynamic with a national vocation in the cyber domain.

... to develop a virtuous cyber virtuous circle ...

- A centre of cyber excellence in Brittany ...

This desire was quickly translated into the establishment of a cyber center of excellence in Brittany, whose creation was announced in the following pages.e by the Minister of Defence in Rennes on 3 June 2013 at a conference organised by the ETRS [7] on the theme "Cybersecurity: a global challenge, a national priority, regional responses". This cluster, although initiated by the Ministry of Defence, goes beyond the military framework alone. It is steered by the region and aims to "federate energies, pool capacities and enable cross-fertilization between experts, teachers and operational staff, military and civilian, public and private". This excerpt from the 2014-2016 Cyber Defence Pact, one of the six major thrusts of which is to develop this centre of excellence for the benefit of the Ministry and, more broadly, the community community, highlights the necessary "win-win" approach inherent in obtaining new, very specific skills. The desire not to centralize all cyber resources in the Paris region, combined with the dense industrial and academic fabric, has thus made the Breton choice legitimate and coherent.

- ... which has three objectives ...

Also, the cyber centre of excellence must allow the creation of a dynamic cyber synergy in the West, not only by bringing new capacities, but above all by enhancing the existing ones. For the sake of coherence, this can only be achieved by developing three areas: training, research and industry. Currently, 2,000 students are already trained each year in Brittany. This figure should increase by 40% in 2015. The aim is to meet a training need through defence/regional partnerships. Research will be complemented by the creation of Breton laboratories, whether in the civil sector, at INRIA [8] in particular, or in defence schools with cyber chairs at ESCC and EN [9]. The budget invested in research should be doubled by 2019. Finally, the development of the industrial sector will be accentuated thanks to the densification of the cyber incubator, a direct consequence of the efforts mentioned and the funding proposed by the region and the State in this field.

- ... through concrete and ambitious projects, both civil and military...

These objectives are already being put into practice in the Great West. The cyber citizen's

reserve initiated in the Paris region, following the report by Senator Jean-Marie Bockel [10], has found a favourable echo in Brittany under the leadership of Major General Boissan, commander of the ETRS. It is working in conjunction with the Cyber Pole of Excellence for the benefit of SMEs and through training to raise awareness and reflect on this field. R&D will be supplemented by the creation of a new centre at DGA MI, operational in March 2016, which will increase the ministry's technical expertise with new platforms simulating a complete environment for virus detection and eradication. The operational area will also be strengthened with the creation, in the summer of 2015, of two new units located in the Rennes region. CALID[11], which already works closely with DGA MI, will have a regional antenna, thus complementing the existing investigation capacities. A cyber-electronic combat company should make it possible to project cyber operational modules in theatres of operation. These entities will be able to rely on the ETRS, which is positioning itself as a major player in the technical training of cyber operators by offering a wider range of training courses. The ESCCs will play a decisive role with the support of these units in their preparation with a cyber range [12], but also in training high-level experts with the specialised master's degree in "cyber crisis management" which will be created at the start of the 2015 academic year and open to civilian students. This synergy is complemented by the dynamism of the region. It is marked by new partnerships with national agencies such as ANSSI[13] for awareness-raising (CyberEdu[14]), by the setting up at ENSIBS[15] of a sandwich course for engineers, unique in France, but also by a closer relationship with the French development sector.fense through the "general partnership agreement" signed on 12 December 2014 with the Ministry of Defence, the CNRS[16] and eleven Breton schools and universities.

Beyond this cyber singularity in a difficult context for defence, this deployment of capabilities is above all the consequence of a global manoeuvre.

... the result of a global approach

- Brittany as a starting point ...

The planned manoeuvre aims first of all to concentrate new skills in Rennes (investigation, technical expertise and projectable units) and to maintain operational capabilities in Paris (steering, planning and surveillance). This regrouping of rare skills, already partially existing in the West, will enable greater reactivity in the face of increasingly significant threats. The objective is not "Paris or Brittany" but "Paris and Brittany". This concentration of efforts will make it possible to create a mass that will benefit the entire nation and even beyond, following the example of what the aeronautics cluster in the Toulouse region has brought to France and the European Union. This cluster is therefore indeed national in scope with an objective of international influence, which justifies the one billion euro effort of the Cyber Defence Pact to carry out the fifty concrete measures that make up this action plan. An effort of coherence is sought to exploit both the skills developed internally while relying on significant R&D capacities in the Brittany region.

- ... a dual approach ...

More and more companies are aware of the dangers and concerned about their own safety. This translates into joint work. The DEFNET exercise, the first of its kind, which was held in October 2014 at the ESCCs, is a good example of this. The objective was to train the Ministry, a specialized crisis unit and three IRMs[17], while working together with the DCI group[18] and two SMEs[19] during this exercise. An attack on the information system

of an air base, a theft of classified data from a radar manufacturer and an attempt to penetrate military networks were simulated. The armed forces, whose action was legitimised by the LBDSN 2013, must therefore not only meet internal needs but also contribute to the defence of the entire nation by helping to improve the protection of administrations and companies. Moreover, the Ministry of Defence, which in the past has been at the origin of technological breakthroughs (use of the third dimension, use of digital technology, development of nuclear power, etc.), has been the driving force behind the LBDSN 2013 project.area), could be, to a certain extent and in close coordination and complementarity with ANSSI, the driving force for new national skills in this dual ecosystem.

- ... which can only be done transversally within the Ministry of Defence

The coherence sought, contrary to what was reported in the media in October 2014, can in no way be achieved by creating a fourth cyber army. First of all because the initial goal is to be as integrated as possible into operations. Since 2011, this objective has been translated into an integrated cyber defence operational chain within the CPCO[20] and under the direction of Vice-Admiral Arnaud Coustillière, General Cyber Defence Officer of the EMA[21]. 21] This centralization would, moreover, run counter to a desire to massively sensitize military personnel. Of the 800 attacks suffered by the Ministry in 2013, a significant part is due to a lack of "computer hygiene". Cyber defence would then only become a problem for specialists, taking it away from the initial objective. Finally, the army model and the current difficulties encountered make it absolutely impossible to envisage such an organisation. The development of these new capabilities must therefore be carried out transversally within the armed forces in order to respond fully to the pressing and differentiated needs of each operational environment.

In short, Brittany, as a regional response to a national priority, appears to be a coherent and legitimate choice. It marks the real awareness of the State to adapt, in a reactive manner, its defence policy to face new challenges and new threats exacerbated by the "Snowden affair", which has provoked a real crisis of international confidence in the use of digital technology.

However, in the face of an ever-changing threat, this effort is from the outset a long-term effort to achieve the international objective identified by the Ministry. Thus, the maintenance of investment, whether human, technical or financial, becomes unavoidable in order to better master this field, which represents a permanent operational and technological challenge.

1] White Paper on Defence and National Security

2] Set of technical and non-technical measures enabling a State to defend in cyberspace the information systems deemed essential.

3] Centre national d'étude des télécommunications, which will become an Orange Labs entity in 2007.

4] SME support scheme for dual innovation

5] Directorate-General for Armaments - Information Control

6] Saint-Cyr Coëtquidan School, Naval School and School of Signals

[7] School of Signals

8] Institut national de recherche en informatique et en automatique (National Institute for Research in Computer Science and Control).

[9] Naval School

10] Information report by Mr Jean-Marie Bockel, on behalf of the Committee on Foreign Affairs, Defence and Armed Forces - No. 681 (2011-2012) - 18 July 2012

[11] Defensive Computer Warfare Analysis Center

12] Training space adapted to this new field of confrontation

13] National Agency for the Security of Information Systems, an agency attached to the General Secretariat for Defence and National Security.

14] Approach led by ANSSI, aimed at raising awareness of computer security among the community of computer specialists who are not specialists in this field.

15] National School of Engineering of South Brittany

16] National Centre for Scientific Research

17] Rapid Response Unit

18] Defence International Counsel

[19] Intrinsec and Acyan

20] Operations Planning and Control Centre

21] Military Staff

Saint-cyrien of the "General Béthouart" promotion (2000-2003), Battalion Chief Arnaud BALLER is a transmitter. He served in the 18th Signal Regiment in Caen and the 41st Signal Regiment in Douai before being assigned to the School of Signals. He is currently doing a Master's degree in Cybersecurity at Supélec/Télécom Bretagne.

Title : le Chef de bataillon Arnaud BALLER

Author (s) : le Chef de bataillon Arnaud BALLER

Release date 18/05/2018