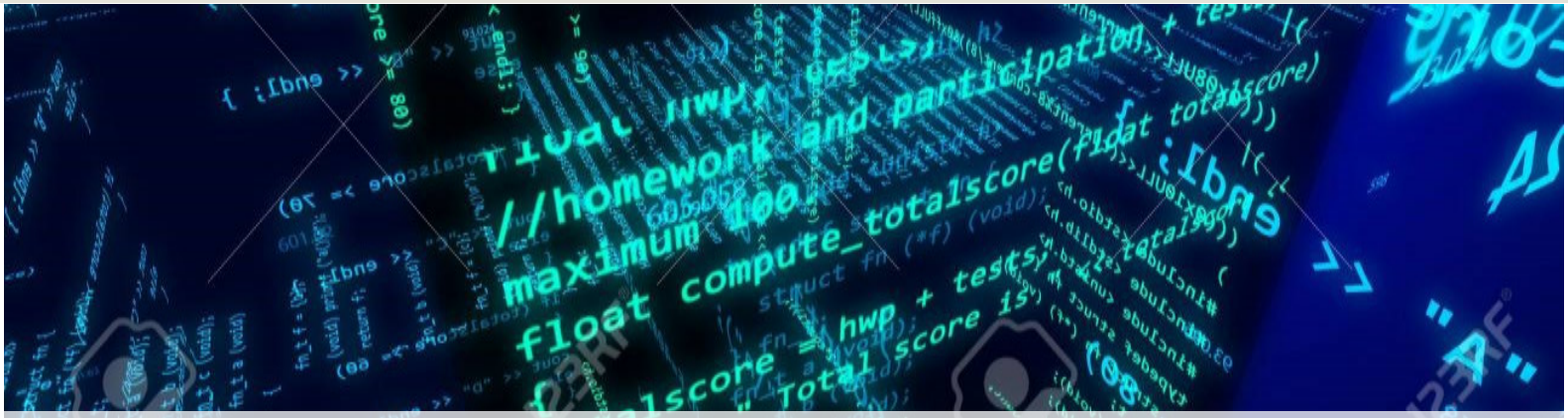

The challenges of cyberspace for the Army

BRENNUS 4.0

le lieutenant-colonel Cheize, de la division doctrine du CDEC

Published on 21/03/2020

Sciences & technologies

Land forces are modernising under the impetus of the "In Touch" reform and the start of the deployment of the SCORPION programme. In the months and years to come, they will have access to major, extremely modern equipment, whether it be vehicles, weapons systems (AS) or operational information and communication systems (OICS). This has led to an overall in-depth reflection on the conduct of operations, between rupture and continuity, with a number of new opportunities offered by these new capabilities. In parallel with this major transformation of the land forces, other challenges have been identified in order to be anticipated now, including the cyber domain.

The cyber environment is a 5th environment in which the army and land forces have been fully involved for several years. This environment [1] is generally divided into several layers (physical, logical and cognitive / semantic).

In order to guarantee his freedom of action in a constantly evolving digital environment, the tactical commander must have the means to assess the digital situation, to assess the situation in terms of the digital situation, toIn order to guarantee his freedom of action in a constantly evolving digital environment, the tactical commander must have the means to assess the digital situation, evaluate the possible consequences on his manoeuvre, defend his systems and, if necessary, obtain or conduct actions [2] in cyberspace in order to ascertain the freedom of manoeuvre of the adversary.

At the tactical as well as strategic level, cyber defence covers three generic functions which are

- intelligence;

- engage;
- defend.

Each of these functions is likely to produce effects that the tactical leader can incorporate as part of his manoeuvre. The effects described in this chapter are generic. Indeed, new opportunities are likely to emerge with the development of technologies and uses.

Expected gains for the Army

The cyber environment remained a reserved domain of the operational/strategic levels until the summer of 2017 as a medium of intervention. Several reasons led to this choice on the part of France. First of all, for political reasons, there is a clear separation of the Defensive Computer Fighting (DF) and Offensive Computer Fighting (OFC) components, as well as, to a lesser extent, the Computer Fight for Influence (CFI). The first component was clearly preponderant over the second, which did not allow for a chain that would have gone down to the tactical levels. Secondly, the steering within EMA/COMCYBER (Cyber Defence Command) was a clear desire to centralise a field in which France wished to control the risks induced by any action carried out in this spectrum. Finally, this new area of operations required extremely rigorous planning, at a pace that did not meet the criteria for responsiveness at the tactical level. This vision changed in the summer of 2017, and the three armies were asked by the EMA/COMCYBER to express their own needs in this area, needs that could not be covered, if need be, by the capabilities held by the strategic level.

Furthermore, the discussions on threat analysis have highlighted one of the specific characteristics of the terrestrial environment, which cannot indeed partition its digital bubble, since its action is carried out within populations, themselves users of digital and radio (electromagnetic) means. Because of this geographical proximity to the potential adversary, land forces can be brought into contact with that adversary, while at the same time being able to act in the same way as they do in the case of a conflict.they are also exposed to hostile action, being able to act locally by means of less sophisticated and low-cost digital actions.

Furthermore, a tactical commander[3] in a land environment is responsible for an area of operations that is increasingly dense in terms of digital systems and the volume of data, stored and transmitted by various communications media, and this trend could continue to grow with ever more efficient means. It must therefore be able to act on this environment in a reactive manner, either to defend its own systems under increasing threat or to seize tactical opportunities by engaging its adversary in or through cyberspace. This paradigm shift is related to several factors, two of which seem to be predominant: observations from the previous day's review of our allies' doctrines, among others, but also the study of recent RETEX tactical operations conducted in part in the cyber environment [4].

At the tactical level, the operational environment includes adversaries capable of conducting local digital actions against which it is necessary to be able to act in near-real

time, which is difficult to achieve at the operational, or even strategic, level from the metropolis.

Finally, the French Army, also seizing the imminence of the arrival of the SCORPION programme, has led a reflection on the conduct of operations in this new infovalorised environment [5] which brings new opportunities, but also new potential threats. It thus seems essential to be able to equip oneself with all the tools for intervention in cyberspace, right down to the lowest tactical levels. The objective is to be able to react to any threat in this spectrum of operations but also to be able to exploit any opportunity to be seized, at a tempo of manoeuvre incompatible with a centralisation of effectors at the strategic level.

The medium-term objective of having such support for land forces is therefore twofold. On the one hand, it is to be able to use this support alone in the framework of the joint manoeuvre, at a given moment in the manoeuvre, in order to fulfil a specific objective. The second is to be able to combine effects within the joint manoeuvre. We speak of the combination of kinetic and non-kinetic effects, for example through the application of depth fire following the geolocation of opposing Ground-to-Air Defense (GAD) radars by cyber units.

Reflections on the expression of Army requirements

On the strength of preliminary conclusions on the expected benefits for the army of investing fully in cyberspace, and of the opening up, at least partially, if not in the framework ofa closer cooperation, from the strategic level, a certain number of reflections have been carried out since the summer of 2017. These reflections have been the subject of studies carried out in parallel with the work prior to the publication of the joint doctrine, Joint Doctrine (JD) 3.20 "Operations in Cyberspace", which established a framework in the cyber environment for the three armies.

Thus, the conclusions of the study entrusted to COMRENS (Intelligence Command) established that a subsequent experimental phase should make it possible to consolidate or modify the choices made.The study's conclusions established that a subsequent experimental phase should make it possible to consolidate or modify the choices made in the DORESE[6] fields, as presented in the study, while particular attention should be paid to the HR pool, which is essential for the implementation of cyber effects. Overall, the cyber-effects[7] could be divided into the three types of generic missions as follows:

The build-up phase for land forces in the cyber environment should enable the command structures of the "In Touch" model to integrate the implementation of cyber effects at the tactical level (in preThe build-up phase of land forces in the cyber environment should enable the command structures of the "In Touch" model to integrate the implementation of cyber effects at the tactical level (in operational readiness, planning and conduct of tactical operations) and on the other hand to enable the SCORPION tactical units, when they are engaged, to benefit from the complementary support provided by cyber effects.

At the same time, the experiments conducted as part of SCORPION VII and IX by the Scorpion Combat Laboratory (LCS) of the Command Doctrine and Training Centre (CDEC) have made it possible, with all the limitations inhéThe SCORPION VII and IX exercises by the Scorpion Combat Laboratory (LCS) of the Command Doctrine and Training Centre (CDEC) made it possible, with all the limitations inherent in simulation and the exploratory nature of these experiments, to define interesting avenues for future capabilities, but also the limits of their implementation. A first limit to a very far-reaching decentralisation of effectors to the lowest tactical levels lies in the intrinsic capabilities of an Inter-Arms Battle Group (IABG) CP, which is not a "battle group", but a "battle group".It is not equipped for such coordination requirements, which is a major focus of attention in this type of operation, both towards neighbouring IATFs and the BIA, and in terms of coordination of the actions of its various Inter-Army Battle Group Sub-Groups (IATGs). The second limitation is that the use of new native support at these tactical levels is contrary to the CPs' desire for agility. The multiplication of Liaison Detachments (LD) within an IATG CP does not seem appropriate when the SCORPION program is precisely seeking, among other expected gains, to be able to accelerate the tempo of the maneuver thanks to increasingly mobile and reactive units. Finally, the last limit is the capacity. A generalization of this type of unit for these levels seems very optimistic at the moment and seems extremely unlikely to be possible in the near future. This scenario would require an exponential increase in the number of effectors on the one hand, but also in the number of specialists who would arm those effectors.

Forward-looking considerations

The multiplication of studies carried out at a very close tempo, and often in parallel, has led to a consideration of this new problem from several complementary angles of attack. The objective is to put land forces in order of battle in the more or less short term in the face of the challenges presented by the presence of this type of unit capable of acting in this new environment which will probably be significantly reinforced in future deployments.

As far as the land forces specifically are concerned, the challenge is above all to be able to seize opportunities. Indeed, the main ones are :

- to challenge the adversary's freedom of manoeuvre, in particular by using all available tools in close cooperation with all the other state actors and to implement and apply the military strategy of influence in cyberspace;
- then, in this space as in others, the main principles of combat have their place, the aim being to exploit any enemy vulnerability detected: mobility, surprise, lightning strikes, concentration of effects are fully applicable; combinations of both tactical and technical innovations will give superiority;
- lastly, all these actions can be combined to support and accompany military operations and achieve the desired effects, as defined by the political authorities, within the legal framework set for force.

Joint operations conducted in cyberspace at the lowest levels of maneuver, they consist

of operations and actions carried out within the perimeter of military cyber defence. CYBER support can be a source of opportunities for the tactical commander [8].

By engaging the neutral and/or ad-verse digital environment through carefully planned and controlled actions, the tactical commander is able to produce and deliver effects that contribute to the execution of the manoeuvre. Indeed, digital actions contribute :

- to the preservation of freedom of action by :

- participating in the collection of intelligence (cyber intelligence);

- providing a defence capability for C2 (Command andControl) and force systems.

- concentration of effort by delivering cyber effects capable of constraining or disrupting the adversary to complement other actions (kinetic and non-kinetic);

- economy of means by disrupting or neutralizing part of the adversary's combat potential before the first contacts or during engagement.

Because of the conditions of access to neutral and ad hoc networks, certain actions can be carried out more effectively from the tactical level (either by means of their own tactical capabilities or by means of capabilities deployed by the strategic level in the theatre of operations). This is particularly the case for cyber actions complementing electronic warfare operations.

In the context of implementation at the TF level, coordination of efforts is ensured by the TSS in the framework of its action plan on the9] in which it is clearly defined that "the Army's ambition is to meet the specific operational requirements of the French Army". cific operational needs of the Army and to this end is based on the guidelines of the Minister of the Army and COMCYBER[10], taking into account all the functions of cyber defence . military defence (LID, "get informed" and "engage" chain) and cybersecurity (cyber-protection, resilience, LID)" . This action plan is based on the operational axes (DORESE) for the next five years, divided into eight main areas of effort.

This new problem for land forces is already taken into account by the CFT in its operational readiness directive, to be published[11] as part of the 5D Operational Preparation (OP), and as such is taken into account at following the RETEX drawn from the experiments of the SCORPION IX exercise in particular, since "the electro-magnetic spectrum (jamming actions of communications systems or radars, GPS jamming) and cyberspace constitute a new area of confrontation. A genuine CI5D (coordination of players in the 5thdimension), following the example of CI3D, ultimately facilitated by artificial intelligence, is indispensable for delivering the right information to the right players at the right time, protecting the environment and protecting the civilian population.It is essential to deliver the right information to the right people at the right time, to protectdata according to their criticality, to avoid information overload, and to obtain complete control of the information (infovalorisation of the SCORPION combat; multiplicity of sensors)" .

The emergence of this 5th cyber environment poses major challenges to an Army that is itself fully focused on its own transformation within the framework of the SCORPION programme. However, it is essential to assert the presence of land forces in the cyber environment in order to be able to deal with all types and levels of adversity.including in this area, potentially carrying threats that may be critical to the integrity of its weapon systems, information systems and communication systems among others [12]. [12] It is also critical to invest in this area because it is also one where an asymmetric adversary might seek to neutralize any advantage that ground forces might gain from infovalorisation, and where a particularly symmetric adversary might seek to neutralize any advantage that ground forces might gain from infovalorisation, and where a particularly symmetric adversary might seek to neutralize any advantage that ground forces might gain from infovalorisation.This, in the context of reflections on the return to high-intensity engagements, contributes fully to the efforts of the TFs to put themselves in order to face tomorrow's threats.

Thus, the cyber capability of the land forces must contribute to the conquest and preservation of the joint commander's freedom of action in and through cyberspace, by providing him with a range of effectors complementary to those obtained through conventional kinetic actions. Whether the tactical mode is offensive or defensive, the concentration of efforts will be manifested in particular by the local and/or temporary production of cyber effects combined with more conventional kinetic actions.

More precisely, in liaison with the various joint commands (COMCYBER, DIRISI, DRM...), the challenge for the Army is to put its land forces in a position where they will be in a position of capability:

- to provide a situation assessment of their own environment, through a Cyber Reference Situation (SCR, or CP);
- to defend their weapons systems, command and control (C2), information systems;
- to identify and request, in support of their manoeuvre, effects that will be produced by higher levels, up to the operational or strategic level;
- produce these effects directly through tactical capabilities that would be deployed within a division, a BIA or even an IATF.

_____

1] As defined in DIA 3.20 "Operations in cyberspace" n°82/ARM/CICDE/DR of 05/09/2018.

2] If these are feasible at the tactical level and authorised by the strategic level.

3] As defined in the study "Tactical Cyber , building a stra-tegy for cyber support to corps and below" published in 2017 by the Rand Corporation, cyber capabilities have been brought down to the level of the Brigade Combat Team (BCT).

4] Case of the operations conducted in Ukraine in 2014, for example.

5] "Exploiting the added value of information resources enabled by new information and communication technologies to improve operational effectiveness" . RFT 3.2.2.1/4 SCORPION Exploratory Doctrine.

6] DORESE: Doctrine, Organization, Resources, Equipment, Support, Training.

7] For the "Inquire" portion of the figure below, the ICR is defined as Cyber Intelligence of Interest and the CAR is defined as Cyber Intelligence of Origin.

8] Developments and experiments in connection with exercises SCORPION VII, IX and X, as well as the work carried out by CO-MRENS in the context of the cyber mandate, have revealed major trends as to what is and is not appropriate to decentralise down to the tactical level.

9] Letter No. 505547/ARM/EMAT/MGAT/DR "Ambition cyber de l'armée de Terre" of 29/05/2019.

10] Letter No. 38/ARM/EMA/COMCYBER of 27 February 2019.

11] DPOFT 2019-2020.

12] DFT 7.2.1 "The generic enemy for the instruction and training of land forces", COMRENS/CDEC, 2019 (being finalized).

Title : le lieutenant-colonel Cheize, de la division doctrine du CDEC

Author (s) : le lieutenant-colonel Cheize, de la division doctrine du CDEC

Release date 17/03/2020

FIND OUT MORE