The conduct of cyber defence operations

BRENNUS 4.0

le Commandant Nicolas Chevrier, du Commandement de la cyberdéfense

Published on 31/03/2020

Sciences & technologies

Since 2013, the White Paper on Defence and National Security states that cyberspace is now a fully-fledged confrontation field, while our strategy is designed to ensure that our national sovereignty can be exercised and respected. Beyond words and the nature of cyberspace, a very tangible reality is emerging where States and powerful groups are assuming the expression of their territoriality in this new space. In this tumultuous context, it is therefore becoming essential for France, and the Ministry of the Armed Forces in particular, to conduct cyber defence operations.

Which confrontational environment for which operations?

As in other fields of confrontation, there is a plethora of different types of cyber defence operations. However, the division of cyberspace into several layers and its transversal positioning in relation to the four traditional environments deserve a few moments of reflection. Thus, it is customary to decompose cyberspace into three levels. The first represents the physical level, i.e. infrastructures such as data centres, network cores or computer cables. The second represents the logical level, which is the data that is stored within these physical infrastructures and how it is formatted and interpreted as it moves through the networks. Finally, the cognitive level, which represents the meaning given to this set of logical information through the content of sites, emails, messages and other content published within social networks.

Thus, it is possible to act within cyberspace but also from cyberspace to the four environments Earth, Air, Sea and Space. From the point of view of the Ministry of the Armed Forces, this amounts to conducting Offensive Computer Response (OCR) and Defensive Computer Response (DCR) operations within a clear legal framework that describes the use of cyber weapons wherever armies are engaged.

In this regard, in its speech delivered in January 2019 on the occasion of the publication by the Ministry of Defence of its LID policy and the doctrine on the use of LIOs for military purposes, the ECS summarised the entire spectrum of military missions according to the triptych "inform - defend - act". It added that the new means of combat (i.e. cyber) could then "combine and, if necessary, replace other military capabilities [...]". Here, it is more interesting to study the combination of cyber capabilities, particularly defensive ones, in support of traditional kinetic operations.

Which battlefield for a cyber defence operation?

In this perspective, it is first of all necessary to identify the area of cyber operations. This phase is particularly complex because it is not restricted to a single environment or geographical area. For example, aircraft are used to carry out an air defence mission over a theatre of operations where other French ground assets are engaged. We could consider here that the area of operation would be limited to the information and communication systems of that theatre. In reality, the subsystems of each of the equipment deployed, from the digitised vehicle to the UAV piloting system and the office automation systems that now equip all the headquarters, are also part of this cyber zone of operations. But more than that, one must also take into account the air base and logistics services from which the aircraft departed and why not a second air base from which any tanker aircraft would depart if the elongation required it. In this connection, there is a notable difference with regard to the definition of an area of operation, generally referred to as an outside area, for kinetic theatres: the cyber battlefield is made up of our own systems. Cyber defence operations are conducted in familiar territory. However, the idea that this would give the defender a considerable advantage, since he or she would be on known ground, must be countered.

First of all, the establishment and maintenance of a relational scheme between operations consisting of different vectors (e.g. reconnaissance drones, aircraft, cavalry squadrons, etc.) and the use of different systems (e.g. airborne reconnaissance drones, aircraft, cavalry squadrons, etc.) is a major advantage.) and knowledge of the very numerous information and communication systems associated with the engagement of these vectors does not exist in a unified manner. Admittedly, the experience and expertise of the operators of these systems gives an idea of this. However, it remains very fragmented, incomplete and not very operational.

Secondly, an operator of information and communication systems will always, in spite of himself, have a certain reluctance to seek out the critical functions of the systems that he is looking for.For fear of calling into question the principles of technical architecture and operation of his system of systems which would lead mechanically to unavailability. These service interruptions are antinomic to the main mission of operators, which is to provide operational users with a service rendered "anytime and anywhere".

Finally, the definition of critical functions differs according to the "mission" or "technical" points of view. Thus, an operator will tend to list, for example, the central servers that perform tasks essential to the operation of the system. While this approach is not entirely wrong, it is not necessarily aligned with a more operational and often detailed reading of the force's mission(s). For example, certain functions such as coordination with allies or ammunition supply are essential to mission accomplishment, but may depend on simple functionalities (software, information portals, etc.). If these were to be targeted, they would not represent a risk to systems in general, but would have a direct impact on mission accomplishment.

Based on this principle, the Atlantic Alliance and the United States, in particular, have developed a doctrine whereby LID operations can be conducted in support of conventional operations with the intention of defending mission-critical systems. This concept is known as Cyber Mission Assurance. However, the defence of these systems does not mean controlling the level of security of those systems. It implies a certain dynamism, a manoeuvre that will allow mission-critical systems (see above) to continue to operate, even in a degraded manner, i.e. under pressure of any kind from one or more adversaries. These are all elements with which it is possible to construct a manoeuvre in response to an aggression. The purpose of the mission is indeed to allow the kinetic operation to continue, even if for this purpose the SCIs identified as essential are maintained and operated in a degraded state of operation.

Conducting a cyber defence operation

A manoeuvre, which is fairly conventional, can thus be developed in three phases: identify/map - deploy - monitor, capable of reacting to an incident.

The first phase, which consists of identifying the famous key elements for a cyber defence manoeuvre, is carried out according to the principles described above. In concrete terms, tasks will be entrusted to operators and operational staff so that together they can search for and identify all these elements, on the basis of a list of ad hoc missions. This may concern: client machines, network interconnections, software (operational or management), dependencies on logistics systems or adherence to third parties, industrial or support services of the Ministry. Taken individually, each of these elements would not have been identified as mission-critical. However, the nature of cyberspace gives the operation a dimension that goes beyond territorial control. Thus, an adversary is able to target a system active in metropolitan France in order to produce an effect against the projected force. Within this framework, each interface and connection with another system should be considered as an access point to be monitored and defended. However, the existence of a permanent cyber posture, based on the model of air defence of the metropolitan territory, provides operational means that need only be supplemented by the LID manoeuvre thus initiated.

In a second stage, surveillance mechanisms adapted as closely as possible to the key elements identified above will be deployed or activated. Before continuing, two points deserve a few moments of reflection. Firstly, a complete phase of the operation will be devoted to the deployment of tools. This is particularly surprising when it is reported in the specialized press, as well as in the more general press, that the immediacy of action is a defining characteristic of cyberspace. In addition and despite the modernity of computer systems, the elements that make them up are not equipped with on-board and automated monitoring mechanisms.

With regard to the first point, the immediacy of action in cyberspace is most often the prerogative of the attacker. The attacker's action, although dazzling, is the result of a long process of targeting [1], of perfecting the tools, backed by solid experience, which enables him to penetrate and then move quickly within the targeted system or systems. For the defender, it is necessary to integrate into the SIC manoeuvre of the operator(s). A high degree of coordination is required as it must not interfere with the day-to-day operation of thousands of other services and tens of thousands of users who function and work perfectly without direct interaction with the operation. However, the assessment of the situation by the command may require a degradation of services beyond the limits of the operation. Here again, the decision of action and its consequences rests with the commanders. It is therefore up to the LID manoeuvre to present its action and possible consequences clearly. This is a serious handicap and one of the reasons why fighting on one's own ground does not confer a tactical advantage over the adversary. The latter will be much more agile and will only be interested in the targets he has chosen, whereas the defender will have to deal with numerous players, often of varying levels of maturity and most of whom are pursuing their own objectives.

With regard to the second point, an analogy with the preparation of tanker aircraft can be developed. For example, an air mission requiring in-flight refuelling does not allow tanker aircraft to be pre-positioned on the runway with their tanks full and waiting for the "mission green", as their taxi gear was not designed to support such a weight on the ground. By way of comparison, the tools that would therefore be deployed during the second phase of the cyber operation are in an identical situation. The effort made to deploy numerous tools that will generate a lot of information and that will require analysis, admittedly automated, but also in-depth investigations at each alert, is not sustainable in the long term. Our infrastructures and cyber combat personnel would not be able to support this effort constantly. It is therefore necessary to find the right balance, deploy the tools and prepare the best possible activation plan.

The third and final phase, "monitoring", is most often the image of cyber defence operations, without knowing what the prerequisites are to get there. The use of all the data collected during the previous phases, in order to try to detect traces of an adversary, is essential. In addition, knowledge of the tactics, techniques and procedures of the adversary or adversaries identified in the mission analysis will complete the picture. Two distinct modes of action can therefore be employed: either "passive" detection, in which conventional and static means of detection will be used, or "active" detection, which consists of "chasing" the adversary. This second mode of action requires an acute knowledge of the battlefield and the opponent's modes of action. The most experienced of them - the adversaries - compete in ingenuity to cover themselves, erase their tracks or hide their actions through exchanges that seem quite legitimate, such as email exchanges, consulting websites with a solid reputation or even through social networks.

Here again, another major characteristic of cyberspace appears. The tempo of the cyber defence operation is generally different from that of the kinetic operation to which it provides support. While the kinetic operation is in a waiting phase, while remaining vigilant, after having identified the means and units that will be used, the cyber operation is busy deploying its device and multiplying the intelligence work on the adversary or adversaries that could threaten the operation. Subsequently, the major effect of the kinetic operation, such as a strike, often marks a decisive condition for the cyber operation. Indeed, the cyber effort is carried out prior to the strikes and continues in a sustained manner afterwards, with a view to possible retaliatory strikes by the adversary or its proxies being conducted in cyberspace.

Fighting against an adversary

Finally, in the event of a cyber offensive action against our system, the switch to a "crisis management" mode must be made in an orderly and organised manner. The first few hours, which are precious, will allow us to collect sufficient information associated with the attack to assess the context, impact, etc., of the attack. Then, the appropriate entities, such as operators, armies or services concerned, will be solicited and involved in order to assess in detail the possible operational impacts, thanks to a grid for reading the operational need or the mission entrusted to them. Coordination, situation sharing and threat assessment are the key to being able to use all the Ministry's defensive levers.

This synthesis is presented to the command, which has its own vision of the events in progress in all the other dimensions and decides on the operational action to be taken in cyberspace (i.e. waiting and characterisation, defending, re-conquering, etc.).

Once the initial situation has been assessed and the players have been alerted, a fairly standard incident response process is set up. This cycle, implemented at the tactical level, can be illustrated according to the principle of an adapted Deming wheel [2].

In the context of an alert, the collection of additional elements to complete the technical assessment is essential. This generally translates into the dispatch of a reduced intervention group whose mission will be, in all discretion, to collect new information. An analogy with the "lightning" mission can be drawn, since at this stage it is advisable to avoid engaging the adversary so that he does not stop his attack abruptly or change his mode of action towards more destructive effects. The next step consists of the analysis and extraction of technical operating elements that will make it possible to detect a possible presence of the attacker in other places in our systems. In this way, new detection capabilities will be implemented, which will make it possible to perhaps find other points of the adversary. This will lead to the collection of new elements and so on...

The whole point of this process is to shorten the execution loop so that the pace of the defender (i.e. OPTEMPO) is shorter than that of the attacker, in order to gradually gain the ascendancy and thus create an opportunity where the initiative can be seized. From then on, the defender will be in a position where he will be able to break the opponent's plan, decide to push him out of the Ministry's CIS and prohibit him from any further action on mission-critical systems.

Operations in cyberspace are a reality. A sharp strategic and tactical sense is needed to adapt to this new field of confrontation... and to win!

1] Or, in some cases, the lack of targeting will be compensated by an inordinate capacity for propagation and replication, as in the Wannacry and NotPetya episodes in May/June 2017. The immediacy of the attack remains real, just a few hours for the whole world to be attacked!

2] The Deming wheel (PDCA, Plan-Do-Check-Act) is a continuous improvement model used in quality management. The Deming wheel is a mnemonic that allows to easily identify the steps to follow to improve quality in an organization.

Title :	le Commandant Nicolas Chevrier, du Commandement de la cyberdéfense
Author (s) :	le Commandant Nicolas Chevrier, du Commandement de la cyberdéfense
Release date	20/03/2020

FIND OUT MORE