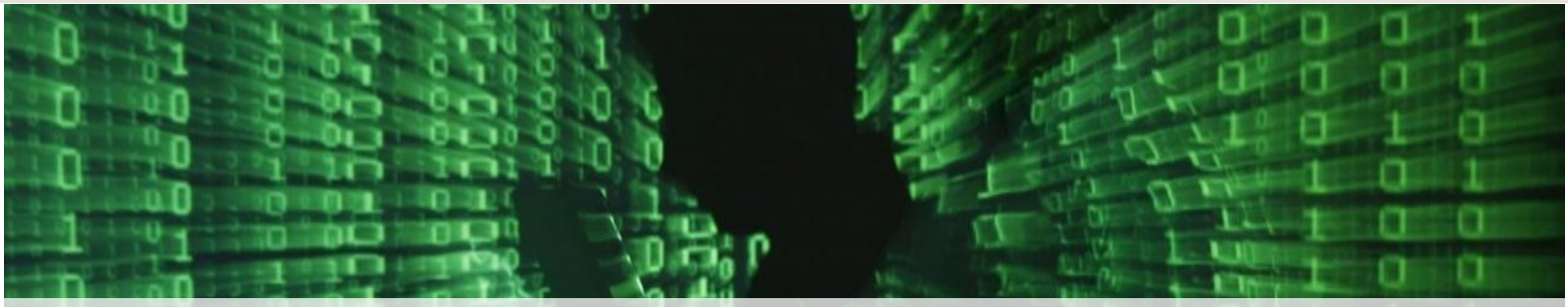

# Cyber defense is first and foremost a fight...

BRENNUS 4.0

le lieutenant-colonel Le Dez, chercheur associé du pôle « Mutation des conflits » du Centre de recherche des écoles de Saint-Cyr

Published on 23/03/2020

Sciences & technologies

**All of today's armed conflicts involve some form of combat in cyberspace. Cyber defence, an often little-known field, allows this digital combat which is today indispensable for domination. We are used to securing our information systems. Cyber defence is fundamentally another mission in a vast digital space. Thanks to action-oriented cyber intelligence, digital combat is planned and conducted by reproducing a known warrior dialectic between attackers and attacked.**

**Cyber defence and security**

The difference between cyber defence and cybersecurity is of the same nature as the more general difference between defence and security in military operations.

Defence is only thought of in terms of interaction with an attacker. It allows the defensive and offensive tactical modes so closely linked.

Security, more global, brings this feeling of being protected: nothing must deprive the leader of his freedom of action, nothing must weaken his protection force. Today, security is framed by directives, regulations, procedures and certifications that are essential to achieve global coherence.

In the digital space, this difference and continuum between security and defence also exists.

Cybersecurity prepares the digital terrain, teams it, cleans it, transforms it so that the fighter is in a favourable situation when he detects the adversary.

Cyber defence seeks contact, the first step in the fight, thanks to cyber intelligence at the end of the action. Once the adversary has been spotted, cyber defence fights to reduce his freedom of action, sometimes beyond our digital front lines, sometimes by actions outside the cyber field. Cyber defence also ends the battle with a stabilization phase, ensuring the transition to those in charge of security. It is a classic conflict after all.

The cyber theatre of operations is much larger than just our computers, it is not just a computer domain. It encompasses all the equipment that contains a little bit of electronics. The abundance of digital objects, connected or not, tends to be the norm in our battlefields. They are military and multiply our combat capabilities tenfold, notably by exchanging data to build an up-to-date operational situation, thus enabling faster manoeuvring and command. This is the digitization of the battlefield.

They are civilian and accompany us on a daily basis in our private lives, which does not stop when we put on our fatigues. These civilian objects are also widely used by our adversaries; small drones or mobile phones are targets of digital combat.

They are industrial and we no longer see them. They allow us to open a door facilitating a commando infiltration, they allow us to thwart enemy surveillance by disrupting the proper functioning of warning devices, they provide information on the use of civilian space by detecting human activities.

Our intelligent electronic space, that of all our weapons systems, our tanks and guns, our vehicles and drones, is not a purely military space. For reasons of cost and ease of development, these military systems today are increasingly being built with the same computer and electronic components that we find in homes and businesses and which are already the target of cyber attacks. This makes the work of the attacker easier, but also of the defence, which operates in familiar territory.

Beyond this digital aspect alone, the cyber theatre of operations also encompasses all the information that circulates there and all the humans who access it. Cyber combat is a battle over perceptions. It uses cyberspace, often far from its technicality, close to its social, informational and media power. It directly affects wills.

Finally, the cyber theatre of operations actually encompasses all electronic equipment: physically exploding a cyber capability into a thousand pieces is the best way to destroy it.

Even if it extends to other fields, particularly industrial ones, cybersecurity is a field fundamentally dedicated to computer specialists, engineers and technicians. They provide a secure resource for command and information exchange without which any victory seems fragile. Fighting against digital pollution, they participate indirectly in the permanent fight against the fog of cyber warfare. Security is all the more indispensable since its aim is to remove, if not reduce, the adversary's freedom of action in our cyberspace. It is therefore a factor of power, one of the factors that make us ever stronger in our cyberspace.

Cyber defence is the domain of digital fighters whose mindset is close to warlike engagement. The digital fighter thinks, organizes, plans and behaves like all the others. It derives principles and knowledge that can be exploited today. Likewise, it is easily integrated into all other forms of combat with still this obstacle, it is a young combat and all in discovery.

Security must be permanent, whereas defence reduced to combat alone is a short phase. As in many things this distinction is not absolute, the preparation and support of its forces tends to give defence a permanent character. Moreover, in our uncertain world, since the threat is constant, the resulting intelligence and adversary search missions are also permanent.

Attack must also be possible at all times. Since digital combat still remains below the threshold of war, it gives leaders the possibility of permanent action to weaken the adversary before acting more violently.

**The indispensable intelligence for digital action**

An intelligence phase initiates any battle. The intelligence makes it possible to establish the order of battle, to characterize the adversary. It is vital to know its numerical form, its modes of action, the traces it leaves or the weapons it uses in order to be able to direct the search in such a vast space. As in land combat, where it is impossible to constantly monitor each route, it is necessary to orient its detection capabilities with static and dynamic search devices.

In defence, the search for the opponent is similar to hunting (the term hunting is the one used by digital fighters). These patrols search on digital equipment for signs of the presence or passage of the adversary. As discreetly as possible, they search memories, hard drives, processors and event logs of all electronic equipment. They analyze abnormal data, files and network flows. Discretion ensures that they do not arouse the suspicions of the adversary, who would be hiding if he knew he was wanted.

Cyber intelligence is the component that enables cyber defence. Without this intelligence capacity for action, it would only be a matter of security which, imagining a theoretical adversary, has no other solution than to act only in conformity with regulatory texts and a risk study that is often dated.

Intelligence is also mandatory for all tactical and operational leaders to take ownership of the subject "fighting in cyberspace". As with all forms of combat, technology (as well as esoteric acronyms) reigns for digital fighters. Often the vocabulary, understanding of the situation or use of weapons is highly technical and sometimes not very intelligible to non-specialists. However, if it remains in its most technical aspect, it is impossible for a command to understand and integrate digital combat, to plan and conduct it in all other forms of land combat. It is necessary to translate technical information such as an IP address (basic information in digital combat, the meaning and stakes of which many readers naturally do not understand) into information from the physical world (a country, a

company, a region, a group of attackers, a machine already used by the adversary in other operations, etc.). This digital/physical transformation is also made possible by tactical intelligence integrated into combat. It is only if this transformation is done that digital combat can escape its self and finally be integrated as a real combat capability. This translation also works the other way around, from a non-cyber command to digital combat.

Embedded in digital combat units, intelligence for action is indispensable for cyber defence to fight in a short tactical cycle. It is impossible to separate this intelligence capability from combat itself; at all stages of combat there is an intelligence requirement.

**The conduct and planning of digital combat**

The search for the adversary is carried out through planned operations with criteria very similar to those of zone control by the army. Based on intelligence, planning sequences the hunt and coordinates the units, details the search modalities (who, what, when, where, how, why, etc.). This may require digital terrain equipment to force the adversary to move towards our detection capabilities (a digital engineering mission), temporarily channel flows or interdict areas to force the adversary to move to facilitate detection. Sometimes it is necessary to ostensibly show some digital deception maneuvers to generate enemy animation.

**The opponent is discovered.**

As in every battle, uncertainty reigns and one should not show that one may have spotted one of these positions.

The opponent is there, we see him, we watch him, we follow him, we try to understand who he really is and what he does, what he wants, what weapons he uses. As long as he does not act against us, we have more interest in clarifying intelligence about him than in revealing our intentions. Above all, we want to know the whole of its apparatus, its entire set-up, its means of communication. Nothing would be easier than to act immediately, nothing would be less effective unless there was a real danger.

We know that as soon as we enter a digital system, the first mission is to multiply the positions and data transmission paths (digital systems are unstable and we must consolidate our attack mechanism). Enemy positions can be numerous and well concealed, dormant and serving as backup. Since the attacker has no alternative but to multiply penetration and exfiltration routes, with different technologies and camouflages, any correction of a vulnerability would only close a door without reducing the attacker. Obviously, if he finds that he has been seen in one place, he will change his tactical mode and he will camouflage his device more deeply. He will always be there, just with tactical modes that are more discreet and therefore harder for the defender to see. He will always be able to act, sometimes brutally when he is no longer visible. To avoid this, the goal for the defender is to know the entire enemy device in order to be able to destroy it.

This intelligence mission on the attacker can only exist if the systems are fully mastered. Again, this is a matter of the security - defence continuum. There are bells ringing to indicate the red lines that the attacker must not cross, actions that he must not take. The planning and the tactical order that follows prepare the response to any change in the attacker's posture. This may involve evicting the attacker even if it has not been possible to discover his entire posture.

But this phase of intelligence acquisition is not only contemplative either. It should make it possible to strengthen certain positions without this being seen as a reaction to an attack. It must also allow the creation of software decoy devices to attract the attention of the attacker and make him reveal his intentions, tactics and techniques. Luring is also informational by intoxicating the attacker, while having him download codes that facilitate the acquisition of intelligence in return. Sometimes the defender must also become the attacker.

A decoy device ("honeypot" simulating equipment or "sandbox" for an entire digital environment) is a simulated portion of digital terrain designed to learn about the opponent's action. The opponent manoeuvres as if it were a portion of our real cyberspace, interacting both with his attacking bases and with other positions in our networks. The defender's goal is to have sufficient knowledge of the opponent's device to cut off all its lines of communication and eliminate its positions in our cyberspace for good. This intelligence mission also requires to channel the enemy into this net by disposing of obstacles elsewhere, in particular stop lines such as network flow filtering devices (a counter-mobility fight). The mission is indeed to mark out the enemy's manoeuvre and gather intelligence in order to bear the cost of the necessary stoppage by making the most of attrition on his combat capabilities. Being able to monitor the adversary at all times without being seen is fundamental, and the camouflage of missions and surveillance systems is essential. As in all battles, the aim is to identify the opponent's weaknesses so that the right force can be applied at the right time to defeat him.

Action-response is a dialogue that takes place between the two belligerents, a game of deception because each believes that its missions have not been detected by the other. The defender is not obliged to stay in his own space. The legitimacy of this fight is to switch at some point to an offensive tactical mode to keep the initiative and be completely in control of the tempo. As in all forms of combat, this offensive-defensive continuum should be the norm in the digital battlespace.

Intelligence, planning, conduct: a cyber defence tactical staff is a "normal" staff so well known in our armies. It is built around these basic functions without forgetting the absolute necessity of having logistics, without which nothing is possible. Thus, it is not difficult to think of its integration in the global military manoeuvre since it follows the principles, the organisation, the will, the warrior spirit.

---

**Title :** le lieutenant-colonel Le Dez, chercheur associé du pôle « Mutation des conflits » du Centre de recherche des écoles de Saint-Cyr

**Author (s) :** le lieutenant-colonel Le Dez, chercheur associé du pôle « Mutation

**Release date** 17/03/2020

FIND OUT MORE