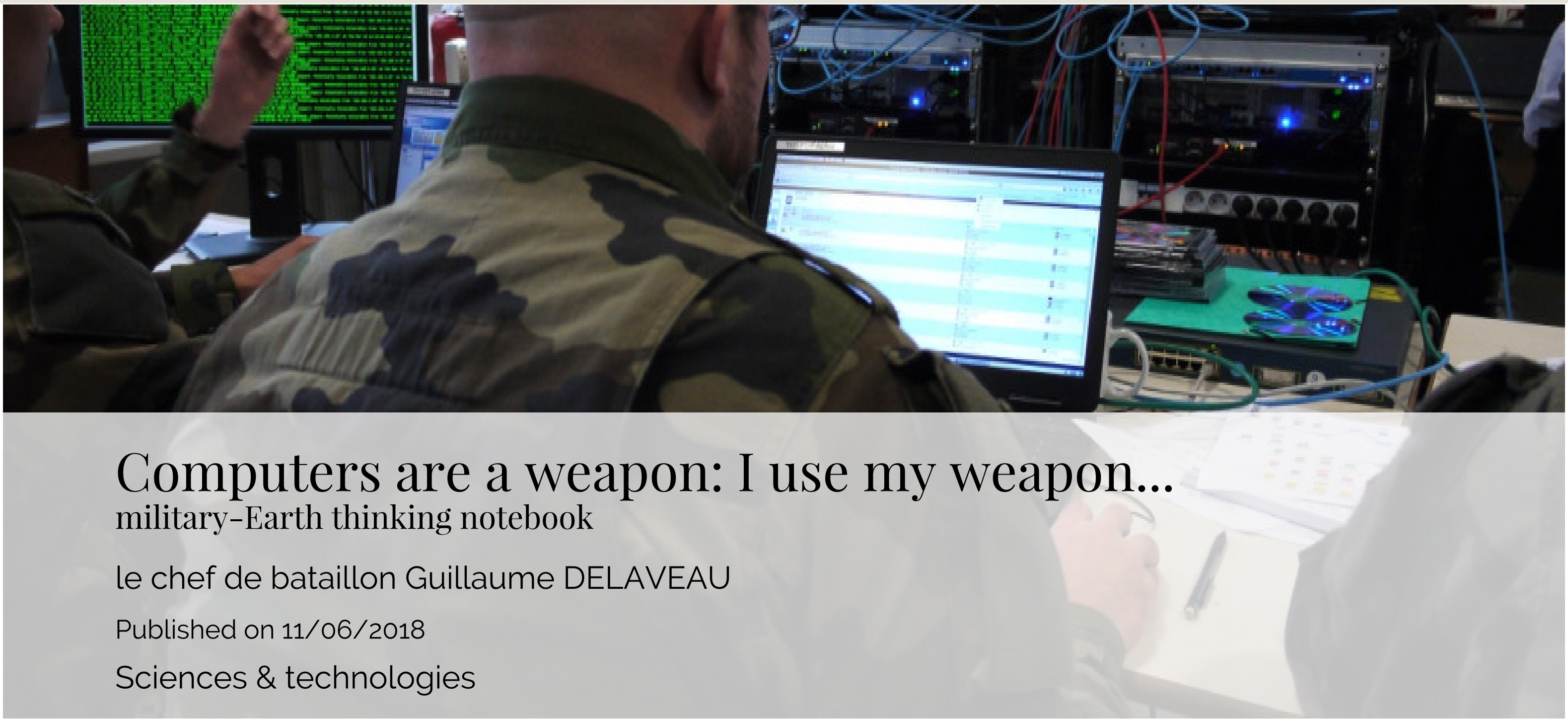

# Computers are a weapon: I use my weapon...

military-Earth thinking notebook

le chef de bataillon Guillaume DELAVEAU

Published on 11/06/2018

Sciences & technologies

**The computer weapon is characteristic of the hybridization of today's conflicts, in which the virtual and physical worlds are no longer hermetic. This weapon has the potential to cause a great deal of damage, including to the adversary. Practicing offensive computer warfare in the forces would greatly facilitate the spread of the cyber spirit and provide France with an additional attack capability, adapted to today's world.**

"One fine morning men will discover with surprise that kind and peaceful objects have acquired offensive and murderous properties".

Qiao Liang and Wang Xiangsui, "War beyond limits»

Russia's offensive in Georgia in 2008 raised awareness among many political and military strategists and leaders. The classic airplane and tank blitz had been preceded by dreadfully effective cyber-attacks.

Since then, France has taken into account the scale of the threat and has set up an operational cyber defence organisation. In a context of budgetary restrictions, the 2013 White Paper even recommends developing cyber defence capabilities. On the other hand, little mention is made of offensive cyber-warfare capabilities. They are cited as a means of characterising the threat and as a "possible option available to the state" [1].

The French preference for the direct approach and the technical aspect of information technology does not encourage the military command to focus on the cyber domain. However, the computer weapon is characteristic of the hybridization of current conflicts, in which the virtual and physical worlds are no longer hermetic. This weapon has the potential to cause a great deal of damage, including to the adversary. So why not train to use it?

An invisible and fearsome weapon

Computer attacks, or cyber attacks, are aimed at hindering the functioning of an information system or stealing information. Since the first one, identified in 1988, they have multiplied, become more complex and amplified.

Historically, the "cyber war" began in 1999, when Serbian hackers attacked NATO intranets to protest the bombings. A real awareness really took place following the paralysis of all administrative services in Estonia in 2007 [2]. The Russian-Georgian conflict of 2008 has given a bellicose dimension to cyber attacks, as the conventional actions of the Russian army were preceded and accompanied by numerous cyber attacks [3].

[3] Eavesdropping, intrusions, destruction, falsifications, taking control of systems: the diversity of hacking operations poses serious threats. Because they have not yet resulted in the death of human beings, they do not have the impact of terrorist acts in public opinion. Worse, hacking[4] offers a contrasting face. Cyber attacks are mostly treated in terms of criminality. They disturb people when their privacy is invaded, but they garner sympathy when the weak attack the strong or the foolish, as evidenced by the actions of Anonymous.

Yet they are a major threat with a high potential impact, especially for a developed state like France. This is the paradox of the strong: the more modern you are, the more dependent you are on your computer networks, and the more targets you offer to potential attackers.

For France, the threat has clearly increased. The multiplicity of systems, their growing interconnection, the complexity of architectures and open source make vulnerabilities more and more numerous and the work of supervision more and more difficult. To the register of threats must be added the particular military use of the radio spectrum: radio links, radio-relay systems, satellite links. This constitutes a significant vector of intrusion. Admittedly, most information systems of the armed forces are partitioned off from the Internet, and when the Internet is used, it is nominally provided by the DIRISI (Direction interarmées des systèmes d'information). But operational urgency or lack of digital hygiene sometimes leads to the adoption of risky behaviours.

Are therefore to be feared: viral infection (of the Conficker type , which has affected armies [5]), intrusion on a network, cyber-aggression after capturing a workstation in a computer system.The Internet has become vital [6] for our society.

6] In addition, the threat of cyber-aggressive states practising active computer-based counter-attack (ACA) is to be taken very seriously. The current recurrence of intrusions (so-called APTs, advanced persistent threats), which require means that only states can provide, suggests that information is methodically collected to make a large-scale attack possible in a conflict situation. The 2013 White Paper states that "by paralysing parts of the country's activity, triggering technological or ecological disasters, such an attack could constitute a genuine act of war" [7]. The discovery of the Stuxnet [8]malicious program in 2010, which attacked the Iranian nuclear program, and then the discovery of the Flame worm in 2012, clearly reflect this new type of confrontation: for strategic purposes, states are conducting a real arms race and increasing the general level of the threat, which has become very professional. The threat is all the greater because computer weapons are proliferating rapidly and with almost total impunity.

France is closing the gap step by step

In parallel with the increase in the threat, the public authorities have become aware of the importance of guaranteeing and adapting information system security (ISS).

In 2008, the White Paper on Defence and National Security enshrined ISS as a "national sovereignty issue". The White Paper for 2013 goes further. It recognises cyberspace as "a field of confrontation in its own right" [9], and announces that a significant effort will be made to improve our defence, detect attacks and be able to "respond adequately" [10].

- From words to deeds

The political will affirmed here first resulted in the creation, in 2009, of the ANSSI, the national agency for information systems security. At the governmental level, this single authority for the protection and defence of information systems has a mandate vis-à-vis the ministries, but also vis-à-vis operators of vital importance (OIVs). The Ministry of Defence plays a key role in this authority, particularly in the event of a major crisis[11].

11] In concrete terms, at the level of the armed forces, an operational organisation has been set up to strengthen the existing functional chain of IS protection. A military doctrine[12] has been promulgated and a cyber command has been put in place. In order to cope with the tempo of the attacks, the unity and speed of decision of a chain of command backed up by that of the conduct and preparation of operations was necessary. This is why the General Cyber Defence Officer, currently Rear Admiral Coustillière, reports to the Chief of the Armed Forces Staff (CAS) [13]. 13] He leads the defensive cyber warfare of the Ministry of Defence and the Armed Forces, and can act through the Operations Planning and Control Centre (CPCO) in the event of a major cyber crisis. It has authority over the Centre d'analyse en lutte informatique défensive (CALID), a veritable specialist armed arm of cyber defence. The CALID, which is in permanent operation, carries out a targeted technology watch, issues and monitors LID measures (defensive IT warfare). It is responsible for steering five of the Ministry's rapid intervention groups, the IRMs [14], which reinforce the first-level groups of the various operators in the event of an attack, and can act directly if necessary. To restore an infected IS, a second level group, composed of 200 specialists, can also be called in as a reinforcement. In addition to strengthening its protection, France has therefore adopted a proactive posture of searching for and detecting attacks, which is known as "in-depth cyber defence".

The armed forces have then applied cyber defence doctrine at their own level.

At the level of the land forces, a directive is thus working to define the functions, resources and conditions of operational readiness for the implementation of cyber defence[15]. However, to date, due to lack of resources, the cyber chain is simply a reinforcement of the existing ISS functional chain, which amounts to giving an operational veneer to the protection of IS. As for the operational preparation, it is in the experimentation phase. The objective is to have trained and projectable cyber modules to counter cyber attacks by 2015.

While French cyber defence is well developed at the politico-strategic level, with France now having a real-time reaction capability and a crisis management capacity, it is not yet developed at the tactical level.

- Marked efforts

Substantial financial and human efforts are being made in cyber defence, but they benefit above all from expertise and intelligence.

200 jobs will thus be created within the Directorate General for Armaments, Information Control Branch (DGA/MI), so that the technical areas of cybersecurity are fully covered. This entity is a reference technical expert, particularly in the field of cryptology. It ensures that the most sensitive components of armament programmes remain under national control and works to develop new technical solutions. At the intelligence level, and by extension in the field of offensive computer warfare[16], the French secret services have strong skills. A supercomputer, the most powerful computer in France, supplied by the Bull company, had moreover made headlines[17]. 17] In terms of training, an effort is being made in three areas: ethical hacking, the ability to respond to crises, and what is known as "forensic", the preservation of evidencefor later analysis. Finally, the Ministry of Defence intends to mobilize the reserve[18]. Alongside the citizen reserve [19], the setting up of an operational reserve, dedicated to the handling of major computer crises, is under study, which appears relevant in this world of networks.

- In search of synergies

France is rightly looking for synergies. The dilution of borders and the strong civil-military duality that characterizes cyberspace make it necessary to strengthen them.

At the national level, government leadership and collaboration with industry and vital infrastructure operators are effective. Similarly, France intends to maintain high-quality academic research. As the training offer does not meet the growing demand for experts, the Ministry of Defence is supporting the project for a cyber defence centre of excellence around Coëtquidan, with the participation of state, academic and industrial players. At the international level, relations are close with NATO, which has emphasised cyber defence in its 2010 strategic concept. France has since permanently joined the Estonian computer centre in Tallinn, NATO's centre of expertise in the cyber field. At the European level, the EuropeanNetwork for Information Security Agency(ENISA), created in 2004, provides useful support to lagging states, but its effectiveness is under discussion because it has no operational responsibility and does not follow a European strategy.

While cooperation in terms of security, in the face of banditry for example, seems possible, disagreements remain profound, particularly over Internet governance, and issues of national sovereignty predominate.

Emphasis should therefore be placed first and foremost on public-private cooperation mechanisms at national level, or even at European level if initiatives materialise, in order to structure an industrial ecosystem that is competent, but too fragmented and financially fragile.

Consequently, the main recommendations of the 2013 White Paper are taken into account: close collaboration with intelligence, upstream research and expertise are taken into account by DGA and the cyber defence organisation is integrated into the forces. France is catching up. It is nevertheless legitimate to question the famous "offensive capabilities that must prepare or accompany military operations" [20]. Naturally covered by secrecy, they should nevertheless be available to tactical and operational leaders for their training, or at least their teaching.

In cyberspace, as elsewhere, the best defence is the attack

The 2013 White Paper announces that offensive capability enriches the range of options available to the State and that it comprises different stages, more or less reversible and more or less discrete, but always proportionate. The message from the authorities at the moment is that if you attack us, you will face a graduated, potentially massive response. This sounds like a transposition of nuclear deterrence into the cyber domain. In this space, however, such a message is not always audible. It is a place where all blows are allowed and asymmetric warfare reaches its peak. France, through its specialized services, is undoubtedly capable of exploiting vulnerabilities, i.e. loopholes unknown to the public. Do our leaders even know that they can use this indirect mode of action prior to any intervention? Would they know how to use the computer weapon to accompany their actions?

The question of the implementation of the IOA, offensive computer warfare, at the tactical and operational levels deserves to be asked.

- Removing the last obstacles

Realism commands to advance towards offensive capabilities. The Bockel report also recommends "pursuing the development of offensive capabilities within armies and specialised services", and questions "the relevance of a public discourse, or even a public doctrine" on these capabilities[21]. 21] For this to happen, it is first necessary to remove certain obstacles, such as the legal blockage. Indeed, the establishment of an IOL capability presupposes the establishment of a doctrine and a framework of employment compatible with the law, in particular international law. The United Nations Charter, the Geneva Conventions and its additional protocols, and the Hague Conventions do not mention IT. They are not, however, inapplicable to cyber attacks, since any legal text is intended to apply to future situations. Similarly, in the law of armed conflict, for a cyber attack as for any other attack, it is the effect that will be judged. It would then be necessary to ensure the application of the usual principles of necessity, proportionality and discrimination[22]. 22] This last principle would be the most difficult to comply with, since most networks are dual-use. But despite some obstacles, such as the inviolability of neutral states, which raises problems with the Internet, international law and the law of armed conflict may apply to cyber attacks. And while waiting for a specific law to emerge, some, like the United States [23], have taken the lead and adopted clear lines. The major stumbling block would rather be of a cultural nature. An army, like any organization, is a man-made system with four components: materials, methods, structures and culture. In French military culture, computer attacks do not seem noble. Tactically, it's all a matter of manoeuvre, in a space-time framework that can be apprehended. Even if there may be cunning, the shock will eventually come. But in cyberspace, the enemy advances under cover. Moreover, many soldiers are still in the process of appropriating, with the risk of rejection, computer innovations. Like any specialist technical field, computing is frightening. As for the ISS, it remains synonymous with constraint and not safety. At the operational level, only electronic warfare is vaguely known [24]. It must be said that our rustic engagements in Afghanistan and Mali are far from the American fantasies of network-centric warfare and RMA, Revolution in military affairs . Yet mistrust is dangerous. Faced with these two blockages, legal and cultural, it would be dangerous to stand still. Let us remember that it was by focusing on defence that our armed forces suffered the heavy defeat of 1940.

- The usefulness of knowing how to attack

In order to move forward in the cyber domain, the IT function must become concrete and attractive. By being attacked and learning how to attack yourself, you can better understand why and how to defend yourself.

It is by making the scenarios of computer attacks credible and by playing them for real that users will learn how to protect themselves. It is also by giving tactical leaders the means to attack with computer weapons with concrete effects that they will then have the reflex to protect themselves and the idea of attacking by this means. For a computer attack can have "field" effects. A convoy of vehicles can have its GPS jammed and get lost, aircraft can get the wrong target, a command post can no longer give orders or, worse, give the wrong ones.

The computer weapon can disrupt enemy communications, mislead decision-makers and give us information. This is the sabotage/espionage binomial, a high-tech version, which cyber-warfare units would offer us.

- How do we do it?

Today, France's offensive computer capability contributes to cyber security and is associated with intelligence capability. To really enrich the range of possible options available to the State, this capability must be developed within the forces. A distinction must first be made between cyberwarfare, information warfare and electronic warfare. Information warfare consists of altering the image of one's adversary, while electronic warfare consists of attack, defence and surveillance in the electromagnetic spectrum. It is only cyberwarfare, which makes it possible to act in the computer or digital realm, that France does not practice completely in the forces.

As far as our allies are concerned, the Pentagon has announced that it is going to increase cyber forces by 3,000, in particular for "offensive digital operations". For its part, the British Ministry of Defence has acknowledged as early as 2011 the existence of units specialising in the creation and use of computer weapons.

The cyber-warfare units of Pakistan, Iran, Syria (the Syrian electronic army), Russia and China are carrying out real media coups that say a lot about their capabilities in the event of conventional conflict. The Chinese People's Army (PLA), without officially recognising the existence of specialised units, has recruited hackers after paying for their studies. 25] and the recruitment and employment policies of cyber units in these countries present us with the dilemma of the three M's: military, militant or mercenary? Standing still on our side gives credence to the proponents of the indirect approach and out-of-bounds warfare.

In France, the creation of cyber-warfare units is not envisaged or claimed. In a context of personnel deflation, it is unrealistic to create new entities in the forces. At the tactical level, it would be wise to start by making better use of offensive electronic warfare, which is already within the prerogatives of the army. The electronic warfare units, whose skills are recognized and whose employment is mastered by the leaders, could be redesigned and reinforced in order to make use of cyber warfare, and in particular jamming [26]. 26] A joint brigade could, as required, obtain reinforcement from units with expanded skills. It is at an operational level, i.e. joint, that specialized units, particularly reserves, could be found. Since cyberspace is a cross-cutting issue, the operational level seems to be the most capable of reacting and acting effectively. It could decide to carry out elaborate cyber-attacks prior to the kinetic attack of conventional forces. It could just as easily carry out mass jamming using a coastal ship as it could be assisted by dedicated cyber units acting from OHQ, the Operative Headquarters, its command post based in metropolitan France, since most operations could be carried out remotely. Cyber attacks can be carried out in several phases, according to the usual methods of planning and targeting. It is easy to imagine an attack on the confidentiality of a network, followed by decryption of the recovered files, which would make it possible to take control of the targeted network and make it unavailable (standby attack).

Cyber-warfare units working and training at a strategic level could therefore descend to the operational level to carry out offensive computer-based warfare in operations and, occasionally, support the tactical level.

France has made great strides in the cyber field. Highly effective in the technical field, it has adequate intelligence resources, has made progress in terms of security and has developed a coherent and robust cyber defence operational chain. The trend is clear: information systems are becoming more and more efficient, virtualized and optimized, and it is becoming more and more difficult to master them at a time when the USA and Asia are establishing themselves as IT superpowers.

Nevertheless, the lack of effective consideration of the cyber threat at the tactical level, and France's timidity regarding the offensive computer battle, do not allow us to be among the most advanced nations in cyberspace. We are therefore not fully aware of the hybridisation of conflicts and we are depriving ourselves of a formidable and essential weapon for our times: the computer weapon.

1] Defence and National Security White Paper 2013, P.105.

2] The attack was claimed by the nachis, a Russian nationalist group, in retaliation for the withdrawal of the Bronze Soldier from Tallinn.

3] In addition to symbolic attacks, such as disfigurements on official sites, Russia disabled the Georgian army's computer system. Georgia's air force was thus grounded at the beginning of the conflict.

4] The term hacking refers to the brilliant young people who, in the 1950s in the United States, seized computers that were then reserved for industrialists and the military.

5] In January 2009, the computer system of the Ministry of Defence was contaminated by this virus. For example, the Navy's Rafales, having been unable to download their flight parameters, remained nailed to the ground.

6] Term used in the 2008 white paper.

7 ] Defence and National Security White Paper 2013, P.48.

8] Stuxnet, which entered Iran via a USB key, infected the SIEMENS software for SCADA (Supervisory Control andData Acquisition), which controls vital industrial infrastructures. While India and Indonesia were also affected, it was Iran that was targeted. According to experts, its nuclear programme has been slowed down by five years due to the deterioration of the centrifuges. Despite the absence of a formal claim, Stuxnet is believed to be the result of extensive collaboration between the United States and Israel.

9] Defence and National Security White Paper 2013, P.45.

10 ] Ibid P 135.

11] This is evidenced by the co-location of their respective surveillance centres, completed in June of this year (COSSI, Centre opérationnel de la sécurité des systèmes d'information, and CALID, Centre d'analyse en lutte informatique défensive).

12] Joint Defence Concept, CIA-6.3 Cyberdef, 12 July 2011 and Joint Doctrine, DIA-6.3 Cyberdef, 7 January 2012.

13] More specifically, Rear-Admiral Coustillière is the Cyber Assistant to the Deputy Chief of Operations at EMA.

14] It should be noted that the Army has a specific IRM, with a projection capability in operation. In international language, we often hear about CERTs, Computer Emergency Response Teams, which are alert and response centres for attacks dedicated to a particular sector. The CERTs are therefore at an intermediate level between CALID and GIR, and correspond to our component COs.

15] Volume 1 concerns the general context, Volume 2, which is entitled "Directive for the Implementation of Cyber Defence in Land Forces" is currently being prepared.It is currently being developed following initial feedback, in particular in order to provide more precise and concrete guidelines (e.g. exercise sheets).

16] Intelligence concerning active computer combat is covered by the Dalia Secret.

17] Its installation, at Alluets-le-Roi in the Yvelines, required the diversion of a high-voltage power line to avoid short circuits in the surrounding villages. The overpowered "bécane" is the delight of young engineers, recruited at the end of school for contracts of three or six years.

18] Speech by Mr. J-Y Le Drian at the opening of the colloquium on cyber defence in Rennes on 3 June 2013.

19] Created in 2012, the cyberdefense network of the citizen reserve has about fifty active members. Its objective is to raise society's awareness of the challenges of cyber defence and cyber resilience.

20] Livre blanc défense et sécurité nationale 2013, P 94.

21] Recommendation No. 10 out of 50 of Senator Jean-Marie Bockel's report, "Cyber defence: a global challenge, a national priority", 19 July 2012.

22] Professor Michael N. Schmitt's 2002 article, "Wire Warfare,computer network attack and jus in bello", is authoritative on the subject. It explains that humanitarian law principles apply from the moment that the computer attack attributed to a state "is intended to cause injury, death, damage or destruction".

23] National Security Directive 16 sets out strict rules of engagement and requires, inter alia, a very high level of approval prior to any attack.

24] Moreover, electronic warfare is mocked for its name, which is said to be overused: "there is as much war in e-warfare as there is sport in e-warfare".

25] Everyone knows each other and has met at the university, such as the famous one from Zhejiang to Hangzhou.

26] To date, one brigade has under its command a light electronic warfare group of less than ten people. This group detects, locates and identifies radio activity, but is inoperable on cellular (GSM) or satellite phones and cannot jam.

Saint-cyrien of the promotion of the "Bicentenary of Saint Cyr" (1999-2002), the DELAVEAU battalion commander is a product of the weapon of transmissions. Head of section at the 41st RT of Senlis, he was projected as SIC advisor to REPFRANCE in Afghanistan and participated in several joint and allied exercises at the operational level. He then commanded a unit at the 48th RT of Agen from 2008 to 2010. Assigned in Bourges in a computer development office, CEDIMAT, he passed the War School competition in 2012.

| | |
|---|---|
| **Title :** | le chef de bataillon Guillaume DELAVEAU |
| **Author (s) :** | le chef de bataillon Guillaume DELAVEAU |
| **Release date** | 23/05/2018 |