A review of the origins of cyberdefense in France

Didier Tisseyre,
general of the Air Force Division, commander of Cyberdefense

Abstract:
Since 2011, the Ministry of Defense and the Armed Forces (in particular its armed wing, the Cyberdefense Command) has built an agile, efficient defense model for conducting operations in the new battle space of the digital realm, where most power struggles, crises and conflicts now have an extension. The armed forces must realize that cybercombat is a full-fledged strategic function that is to be combined with other global maneuvers. Combat in cyberspace is inherently asymmetrical, mixed, sometimes invisible and apparently painless. Nevertheless, cyberweapons can seriously damage the capacities and interests of sovereign nation-states. To protect, defend and act when faced with such menaces, the government's determination and the passage of successive program acts for the armed forces have enabled France to build up its cyberdefenses. Faced with adversaries, enemies, or rivals equipped with an offensive capacity in information systems, France's ambitious plan of ministerial actions, based on a new doctrine and organization, enables our forces to be deployed and conduct digital combat. This was taken a step farther in 2017 with the creation, by decree, of COMCYBER, the Cyberdefense Command. Cyberdefense is still a top priority for the Ministry of the Armed Forces, the goal being to endow France with the means for building a tool on par with its operational ambitions and to fully ensure the country's cybersecurity. On 3 October 2019, the Ministry of the Armed Forces inaugurated in Rennes the first building fully devoted to cyberoperations, this being evidence of a trend that will enable France to stand out thanks to its status as a cyberpower.

Fifty years ago, in 1969, the US Defense Advanced Research Projects Agency (DARPA) set up ARPANET (Advanced Research Projects Agency Network) for the American armed forces. Twenty years later, ARPANET yielded to the Internet and then the World Wide Web. The digitization of the world thus came to revolve around the vastest artificial "object" designed by mankind in the 20th century: cyberspace. This space is a new, constantly evolving realm of innovation and confrontation.

This new network needed to have solid roots to continue growing, while seeing to its security and protection. Given its continually evolution, the Internet requires an agile approach and a thorough overhaul of our organizations and a realignment of forces. Since 2011, the French Ministry of Defense (later of the Armed Forces), in particular its armed branch, the Cyberdefense Command, has been building an agile, effective model for a solid, durable cyberdefense.[1]

Cyberspace has its own momentum, impelled by an expanding, apparently boundless technology: yesterday, interconnecting networks; today, augmenting the computational power for data processing; tomorrow, the proliferation of connected devices; the day after tomorrow, quantum processors. The Internet is probably humanity's most innovative technical revolution. This source of wealth is a vector of knowledge and of new cultural and business models. It shortens

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in February 2020.

distances and brings individuals together. Our society's center of gravity, which used to be mainly related to the population and territory, is gradually moving into this new space. The dependence on electronic technology is growing at the pace of technological progress, thus increasing our exposure to new risks and making us vulnerable.

Most contemporary power struggles, conflicts and crises will systematically have prolongations in cyberspace. The armed forces must address the issue of cybernetic combat as a full-fledged strategic mission with effects that will be added onto the other effects in global maneuvers.

A new battlefield

Cyberweapons signal a technological turning point with respect to the use of force. They are going to disrupt forms of warfare but without deeply altering its principles. A host of state-sponsored forces (whether masked or not), terrorist or criminal organizations who rapidly spread, leap over borders, blur our perceptions, make us lose our bearings, and flout international law and basic rules of behavior… all these are risks in cyberspace — a foggy, gray zone with a quite real, sometimes devastating impact. Combat in cyberspace is asymmetric, hybrid, sometimes invisible and apparently painless. Nonetheless, cyberweapons are capable of seriously damaging a state's sovereignty and interests.

We can point to four major categories of cyberthreats:

- the damage to one's image: the defacement of official websites, smear campaigns, the usurpation of identifications, propaganda, the amplification of rumors, acts of destabilization, etc.;
- criminal actions: credit card scams, ransomware, rackets of all sorts, etc.;
- espionage: the stealthy misappropriation of information circulating on a target's digital networks; and
- sabotage: hacking a system to alter its operation.

These threats in cyberspace have the same characteristics as the threats in physical space: malevolent individuals who prepare terrorist actions, disseminate disinformation, use baits, steal or even destroy. The boundaries between actors — cybercriminals, hacktivists, states, terrorist groups, etc. — are porous. The variety of threats is very broad, ranging from attacks on electronic voting machines to a paralysis of the media or the outage of an electricity grid. Underlying these scenarios are deeply asymmetric situations: the use of small means for a strategic impact (similar to more conventional actions), in particular when they are aimed at the critical civilian infrastructures or crucial military installations on which our sovereignty depends.

The frequency and scope of cyberattacks are continually increasing, evidence of this being the troubling proliferation of the means of aggression. Although few states yet have the means for conducting large-scale cyberoffensives that would inflict major damage, it is very likely that more states will soon develop this capacity — given the low costs and rapid dissemination of new forms of digital technology. Furthermore, a state might have to allot colossal means to design its cyberweapons, but the latter can be duplicated easily and are likely to be copied. Terrorist groups, who already use the Internet to plan actions, disseminate propaganda and muster recruits, might become full-fledged fighters in this new realm. After all, it is very hard to determine the origin of attacks.

A rapid change of scale

To protect, defend and act, France has built its cyberdefense on the government's determination and the place of this issue in successive armed forces program acts. To confront adversaries, enemies or competitors equipped with an offensive capacity in digital technology, an ambitious ministerial action plan has been worked out. It is based on an updated military doctrine and organization so that our armed forces can be deployed to cope with menaces and undertake cybercombat.

The 2008 white book on national defense and security mentioned, for the first time, threats related to the development of cyberspace.[2] ANSII (Agence Nationale de la Sécurité des Systèmes d'Information) was created in 2009; and then in 2011, the position of general officer of cyberdefense on the staff of command of the armed forces. During the next eight years, cyberdefense was continually adapted to operational situations. The 2013 white book on national defense and security stipulated that, as part of the national doctrine, an offensive cybercapacity, in association with the intelligence, was significant for the positioning of cybersecurity.[3] The 2014-2016 Cyberdefense Pact mustered the Ministry of the Armed Forces around the objectives of making France a major military power in cyberdefense and of creating a national cyberdefense community. This announced "*change of scale*" drew attention to the need to industrialize France's military cyberdefense. In October 2015 the Center of Operations of Cyberdefense (CO-CYBER) was set up with the assignment to plan and conduct military operations in cyberspace.

The road taken for a decade now is proof of the stakes. It reflects France's ambition to become a big cyberpower.

The Cyberdefense Command: COMCYBER

Thanks to this change of scale, a very important symbolic threshold was crossed in 2017 when a decree provided for setting up the Cyberdefense Command (COMCYBER, Commandement de la Cyberdéfense). As part of the staff of command of the armed forces, COMCYBER is the key unit that oversees military operations in cyberspace. More recently, the *Revue stratégique de défense et de sécurité nationale* in October 2017, the *Revue stratégique de cyberdefense* in February 2018, and the 2019-2025 armed forces program act of July 2018 have all made military cyberdefense a major issue. They have increased its visibility and devoted more financial and human means to it.[4] On 18 January 2019, France, through the minister of the Armed Forces, publicly recognized that cyberoffensives are now part of the arsenal that can be used against an enemy, whether or not in response to a prior act of aggression.

To defend national sovereignty in cyberspace, the Ministry of the Armed Forces is capable of protecting itself from computer attacks, detecting them and identifying the perpetrators. It is also capable of exploiting flaws in an enemy's information systems during confrontations and exercising a command over all aspects of digital combat.

[2] *Le Livre blanc de la défense et de la sécurité nationale de 2008* (Paris: La Documentation Française), 124p., available via http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf.

[3] *French white paper: Defense and national security 2013* (Paris: Ministère de la Défense), 137p., available via https://www.defense.gouv.fr/content/download/215253/2394121/White%20paper%20on%20defense%20%202013.pdf.

[4] http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/.

Like the Special Operations Command, COMCYBER is placed directly under the authority of the Armed Forces' chief of staff. The decree creating it stipulated that it is in charge of the protection and defense of the Ministry's information systems and of conducting digital actions against enemy systems.

Cyberprotection means building thick walls around information systems and permanently testing their effectiveness so as to be capable of dealing with an ever evolving threat. Defending these systems is a dynamic activity complementary to protecting them. Defense involves patrolling, watching and monitoring information systems and intervening during attacks in order to eradicate threats and rebuild walls. State authorities have a wider range of options about the digital weapons to use for offensive actions. Cyberspace has become a place of full-blown confrontations just like the seas, land or air and, more recently, the space above the Earth's atmosphere. Military operations cannot be designed without taking account of this new dimension.

This command has been built on the rationale of an economy of forces so as to pool skills and concentrate efforts, and on the model of a network, like the material and immaterial spaces where COMCYBER launches actions. This allows for beneficial interactions in digital technology among stakeholders, whether governmental or private, and for controlling actions through specific functional channels. The French cyberdefense model has kept an eye on societal trends. For citizens who use cyberspace, the Ministry of the Armed Forces is an inspiration, a source of confidence and security — the place for the creation and emulation of cyber-resilience. COMCYBER wants to be a federating force in the Ministry that conveys a message about reinforcing interministerial capacities.

Defense in France and Europe has to adapt to current and future issues on this digital battlefield. The operational superiority of our forces — the capacity for controlling crises and being the first on the theater of conflict to effectively counter an enemy — now means looking for, and exercising, superiority in cyberspace. For this reason, cyberdefense in the Ministry of the Armed Forces has been thought out in terms of actions and designed in line with the reality of the modern world, which is already undergoing its digital transformation.

Nearly 3400 cybercombatants, distributed throughout the armed forces and various services in the Ministry, are placed under the authority of COMCYBER's general officer, who is backed by an operational staff of approximately seventy persons organized around four poles.

The Ministry of the Armed Forces and COMCYBER have a special place in organizing the nation's cyberdefense. This organization is based on the principle of a separation between defensive and offensive actions. It involves three major partners who work with COMCYBER: ANSSI along with the general directorates for external and internal security (respectively DGSE and DGSI). ANSSI handles questions of defense at the governmental level. The Ministry of the Armed Forces, via COMCYBER and in full coordination with ANSSI, sees to the defense of its own networks. Furthermore, it can come in reinforcement to ANSSI if this agency asks for its assistance during major cyberattacks against our country. The offensive means for cyberdefense are in the hands of COMCYBER, along with other organizations. Under the authority of the head of the Armed Forces, COMCYBER oversees the use of cyberoffensive means during military operations.

COMCYBER also relies on a system of international partnerships. As in all sensitive matters (intelligence and special operations), which are necessarily subject to secrecy, cyberdefense is, nonetheless, a field where international exchanges, often bilateral, are possible, if not indispensable. This cooperation takes various forms, ranging from an exchange of good practices to procedures for information-sharing (thus enabling COMCYBER to improve its knowledge of a situation and of threats) and even the execution and coordination of joint operations within the red lines set nationally. This cooperation is a key to knowledge, operational effectiveness and COMCYBER's influence within the international military community of cyberdefense.

The prospects

The upgrading of cyberdefense is continuing. The change of scale, as mentioned, is still taking place; and several challenges are yet to be taken up.

First of all, the issue of human resources must be addressed; it is one facet of the global challenge of the digitization of the Ministry of the Armed Forces. The cybercombatants whom the Ministry needs to operate in cyberspace on a level equal to the threats against us have to be recruited and trained. Their recruitment and retention are a major issue in all big organizations. The shortage, whether structural or cyclical, of talent has created the conditions for stiff competition in a bullish labor market. To cope with this situation, the public administration, in general, and military cyberdefense, in particular, have proven to be inventive so as to attract the attention of young graduates and to arouse and sustain in them an interest that might eventually lead to working together for a relatively long period. To be clear: the private sector has the advantage of offering more interesting pay prospects. However the public sector has the advantage of offering a stimulating work environment based on the quest for effectiveness and not bound by sales targets, in other words an environment conducive to technical excellence. Furthermore, it offers the occasion to concretely serve one's country and acquire a solid, widely recognized experience.

Training cybercombatants is also a major challenge. Current training models have to be overhauled throughout the armed forces' digital community. A new model is to be designed, one better adapted to current, real-life situations and to what we can glimpse of tomorrow's reality. The Ministry must be sure to have on hand the human resources qualified in cybersecurity whose skills will be constantly upgraded to the highest technical level. This objective calls for making the efforts of everyone in the Ministry converge. Internal coordination has to be bolstered. A center of expertise on the training and careers of cyberprofessionals at the Ministry of the Armed Forces must be set up, in short a "cyberacademy" that could be the brick for working out a general solution to this problem. The Ministry's assets can be put to use for training purposes.

Finally, cyberdefense also faces a technical challenge unlike in any other field. No other field has undergone a rotation as fast as digital technology. At each instant, it is necessary to be familiar with all trends — those already accomplished and, if possible, those that will soon play out — to be proficient in techniques and to train all the personnel needed to master these techniques on a large scale. Several issues will crop up in the short run, for instance the acquirement of a capacity for hypervision (in contrast with supervision). In the middle run, artificial intelligence will have to be used to detect threats and react to ever more sophisticated acts of aggression. In the long run, quantum computing could signal a major break, namely a massive, complete and definitive shift from the classical encryption used in cybersecurity.

Conclusion

For the Ministry of the Armed Forces, cyberdefense is still a top priority. The aim is to endow France with the means for making tools on par with the country's operational ambitions and to vouchsafe cybersecurity.

On 3 October 2019, the minister of the Armed Forces inaugurated in Rennes a building devoted to cyberoperations. This building, part of a technological cluster in Brittany, is very close to the Cyberdefense Factory, a subsidized incubator of cybersecurity companies. This trend will enable France to shine its light and attain the status of a cyberpower.