Unofficial translation of “Éléments publics de doctrine militaire de lutte informatique offensive”
by **S**wit**H**ak | Twitter: **@S**wit**H**ak | January 2019

Public elements of French military doctrine of offensive computer warfare

Translator's note:

This is an **unofficial translation** of the original publication by the French Ministry of Defense document “Éléments publics de doctrine militaire de lutte informatique offensive”.

The **original** document in French is available online:
https://www.defense.gouv.fr/content/download/551531/9394285/Politique%20MINARM%20de%20lutte%20informatique%20OFFENSIVE.pdf

SUMMARY

1. PREAMBLE 3

2. ACTING IN CYBERSPACE: offensive computer warfare for military purposes, a weapon of operational superiority 4

3. CONTROL OF THE RISKS RELATED TO THE USE OF THE LIO: a sine qua non condition of any operation 7

4. LEGALLY FRAMING LIO ACTION: a necessity and a protection 8

5. DEVELOPING A SHARED LIO CULTURE: Effects to be integrated in a coalition 8

6. FACING A CHALLENGE FOR THE FUTURE: the LIO, a military employment capability to be developed 9

PREAMBLE

Nuclear, conventional and cyber military power, permanent member of the Council of the United Nations, the Atlantic Treaty Organization and the European Union, France assumes, under the authority of the President of the Republic, its commitments on the international scene. In an environment where geopolitical crisis, destabilization, terrorist threat and conventional and hybrid wars, the Ministry of the Armed Forces contributes to guaranteeing, in all circumstances, in times of peace or war, France's national sovereignty and decision-making autonomy, both on national territory and in all the external theatres where our armies are deployed.

The cyber-attacks against Estonia in 2007, against the electricity grids of Ukraine, against TV5 Monde in 2015, the WannaCry ransomware in spring 2017 or the NotPetya attack in June 2017, illustrate the possible fields of action for attackers whose four major objectives are espionage, illegal trafficking, destabilization and sabotage.

Most contemporary power struggles, crises and conflicts are developing in the digital space. Armies must now systematically view cyber combat as a mode of action in its own right, the effects of which are combined with others in a global movement.

A real breakthrough in terms of technology and the use of force, the cyber weapon is to disrupt the modalities of the war without profoundly renewing its terms principles. Multiplicity of state actors, masked or not, terrorist organizations, erased boundaries, disturbed perceptions, distorted landmarks, rapid spread, law international non-compliance, a broken code of conduct: these are the risks of cyberspace.

A grey area, a fog, whose effects are very real, sometimes devastating.

The fight in cyberspace is asymmetrical, hybrid, sometimes invisible in nature and apparently painless. However, the use of cyber weapons is likely to carry seriously undermining the sovereign capacities and interests of States.

The strategic review of cyber defense, published in February 2018, confirmed the relevance of our organizational and governance model that separates offensive missions and capabilities from defensive missions and capabilities. It has proposed a full-fledged strategy in this area by structuring the organization of cyber defense around an inter-ministerial cyber crisis coordination center run by the General Secretariat for Defense and National Security (SGDSN) under the authority of the Prime Minister and four separate operational channels. In addition to the "protection", "intelligence" and "judicial investigation" channels, the "military action" channel uses offensive computer warfare (LIO) in particular.

France is thus consolidating a renewed model of cyber defense, of which the creation of the Cyber Defense Command (COMCYBER) in May 2017[1] was one of the founding steps within the Ministry of the Armed Forces. The COMCYBER is responsible for military cyber defense, which covers all defensive and offensive actions conducted in cyberspace to ensure the proper functioning of the ministry and the effectiveness of the armed forces in preparing, planning and conducting military operations.

From now on, the Ministry of the Armed Forces has capacities and a doctrine of employment that cover cyber-offensive actions dedicated to the engagement of the armed forces.

[1] Decree N° 2017-743 of 4 May 2017 on the powers of the Chief of the Armed Forces Staff and the Decision of 4 May 2017 amending the organization of the Armed Forces Staff

ACTING IN CYBERSPACE: offensive computer warfare for military purposes, a weapon of operational superiority

The ability to conduct defensive and offensive military operations in the cyberspace helps to guarantee national sovereignty. It participates in obtaining operational advantages in the operational areas of our armed forces, but also to the defense of the armed forces' information systems. Thus, the armed forces are now equipped with the full spectrum of computer control resources necessary for the conduct of operations: defensive, offensive and against manipulation information that is harmful to our military operations.

Under the authority of the Chief of the Armed Forces Staff, the COMCYBER is the employment authority of cyber offensive military capability, an integral part of the operational chain of armed forces, in perfect coherence with their organization and operational structure.

1) OFFENSIVE COMPUTER WARFARE FOR MILITARY PURPOSES: AN AGILE AND INNOVATIVE CAPABILITY

The offensive computer fight for military purposes (LIO) covers all actions undertaken in cyberspace, conducted autonomously or in combination with conventional military means. The cyber weapon aims, in strict compliance with international rules[2], to produce effects against an enemy system to the purpose of altering the availability or confidentiality of data.

The variety of effects of the LIO and the corresponding modes of action are due to the nature of cyberspace, a new field of confrontation. It is based on a three-layer structure:

- a physical layer, consisting of the equipment of computer systems and their networks having a material existence and, for some of them, an electromagnetic existence (computers, processors, cables, fibers, transmitters, receivers, satellite links, routers, etc.);

- a logical layer, consisting of all digital data, processes and tools for managing and administrating this data, as well as their exchange flows (files, sites, addresses, connection codes, protocols, software, applications, etc.), implemented inside the hardware to enable them to provide the expected services;

- a semantic and social layer, made up of information that circulates in cyberspace and people who may have multiple digital identities or " Avatars " (nicknames, mail addresses, IP addresses, blogs, etc.).

The interdependence of these three layers reinforces the opportunities for action by the LIO and therefore destabilizes the opponent.

When combined with conventional modes of action, the LIO takes full effect potential multiplier dimension of effects - amplify, improve or complement. She benefits particularly from the increasing networking of all systems military, as well as their interconnections with the Internet.

The use of the LIO is part of a time frame of its own. If its effects can to be dazzling, its integration into the overall operational movement is a major factor in a process characterized by a long and very specific planning. These effects may be of a material nature - neutralization of a weapon system - or intangible - collection of information, temporary, reversible or definitive.

[2] As specified in the Cyber Defense Strategic Review, these rules define, in particular, the conditions for the triggering or application of retaliatory measures, countermeasures or even the use of force in the event of armed aggression justifying the use of legitimate self-defense.

2) THE AIM OF THE LIO: TO CONTRIBUTE IN CYBERSPACE TO MILITARY SUPERIORITY

In the face of an adversary, the LIO offers discreet and effective modes of action against digital systems, capable of substituting, preparing or complementing other modes of action.

The LIO makes it possible to take advantage of vulnerabilities in adversary digital systems during all phases of a crisis: intelligence, prevention, management or stabilization.

It makes it possible to achieve three types of operational objectives in the conduct of military operations:

1) assessment of adverse military capabilities: information gathering or extraction;
2) reduction or even neutralization of enemy capabilities: temporary disruption or creation of major damage to enemy military capabilities;
3) modification of the adversary's perceptions or analytical capacity: discreet alteration of data or systems, exploitation of stolen information within an adversary's military information system.

The targets may be exposed on the Internet, isolated, or an integral part of a more global weapons system. The IOL contributes to the security and even preservation of the digitized means used by our deployed forces. LIO's actions are not necessarily led to physical contact with the opponent.

The LIO can also support defensive computer warfare when the computer attack is aimed exclusively at the operational capabilities of the or defense chains of command by participating in the characterization of an attack, by stopping a cyber-attack on our systems, in accordance with Article L. 2321-2 of the French Defense Code[3] or by imposing a diversion of his efforts to unnecessary targets.

Complementary to conventional weapons, the IOL produces the same intelligence, neutralization or disappointment effects while operating in a new field.

It can be used as a substitute or in combination with other collection or action on the entire spectrum of military engagement: intelligence, defense, act:

PLACE OF THE LIO IN OPERATING FUNCTIONS

INTELLIGENCE	DEFENSE	ACT
Characterize and assign adversary systems	Identifying the attacker	Counteracting misinformation
Watch the opponent	**Retaliate.** Intervene in the cyberspace in case of intrusion	Accompanying the military operation by disrupting or neutralizing the adversary's military capabilities
	Neutralization in accordance with Art. L. 2321-2 of the French Defense Code	

[3] Article 21 of Act No. 2013-1168 of 18 December 2013 on military programming for the years 2014 to 2019 and various provisions concerning national Defense and Security.

3) THE ORGANIZATION OF THE LIO: A UNIFIED CHAIN OF COMMAND, SPECIALIZED UNITS

The LIO is based on sensitive know-how and is one of the attributes of a sovereign defense. These two dimensions require strategic control of LIO operations, from planning to implementation.

Under the authority of the President of the Republic and at the direction of the Chief of the Armed Forces Staff, the COMCYBER is responsible for planning and coordinating LIO operations for the benefit of the joint operation. It ensures the consistency of the planning and conduct of LIO actions with the various operational headquarters (joint, land, naval, air, special forces), and intelligence services, from the strategic to the tactical level. Finally, he develops and leads the LIO component of military cooperation with allies.

The use of the LIO is conceived at the strategic (in the global joint operational exercise) and tactical (in the operation of the army components on the operation theaters).

EXAMPLES OF THE USE OF LIO AT THE TACTICAL LEVEL AND AT THE STRATEGIC LEVEL

	Tactical-level employments	Strategic-level employments
Assessment of adversary capacities	- Intelligence of immediate interest related to the action of the forces	- Intelligence in preparation for operations, for targeting or capacity development purposes
Reduction or even neutralization of adverse capacities	- Neutralization of a weapon system - Neutralization of a commandment post	- Neutralization of an adverse operational capability (example: propaganda vector), - Neutralization of a strategic level commandment-level system
Action on perceptions or adverse analytical capacity	- Alteration of data in a commandment system	- Disorganization of enemy propaganda centers

LIO's operations are conducted by specialized units, whose expertise guarantees risk analysis and the control of collateral and even fratricidal effects induced by the complexity of the field. The action of these specialized units is fully integrated into the army's operations, either directly in the field or remotely.

CONTROL OF THE RISKS RELATED TO THE USE OF THE LIO: *a sine qua non* condition of any operation

At the command of General Officer COMCYBER, the use of the LIO requires a command of the political, legal and military risks in all phases of the operation.

Like any military operation, the LIO implies an acceptance of risk by the military level. decision-making, determined by the principles of jus in bello (proportionality, distinction, discrimination, …), cost-effectiveness, operational situation and context general policy.

The risks associated with the use of the LIO are primarily due to the following characteristics specific to cyberspace: immediacy of action, duality of targets and hyper connectivity.

In addition, the sophisticated means and modes of action designed to carry out these actions require strict control and monitoring of their use from start to finish in order to avoid any risk of misappropriation, compromise or collateral damage. Indeed, an action by LIO can spread its effects beyond the target due to configuration unknowns and interdependencies between systems, increasingly common in cyberspace. In addition, a LIO tool may be stolen, copied or imitated by opponents or third parties. It does not present generally not the constraints associated with threshold weapons reserved for States with a certain technological maturity.

Finally, opponents with offensive capabilities, but who would provide a surface of lower digital vulnerability could engage at lower risk in a conflicting escalation against our interests.

To preserve its effectiveness and control the risks of diversion, all the LIO operations conducted by the armed forces remain of a secret nature, but the political and military authorities may, depending on the circumstances, assume them publicly or even claim them. This posture is a matter of political decision. The decision to make a LIO action public must, in the end, be weighed against the risk posed by the vulnerability inherent in the high level of digitization of our interests national.

LEGALLY FRAMING LIO ACTION: a necessity and a protection

The LIO is subject, like any other weapon or method of warfare, to the principles and rules of international law, including international humanitarian law, as well as national laws and regulations. It is therefore only used in accordance with very restrictive operational rules of engagement.

When carried out in support of the defensive IT fight, the actions of LIO are conducted, under the responsibility of the Chief of the Armed Forces Staff, in the framework defined in national law by the Defense Code and under the conditions laid down by the Prime Minister.

France is seeking the adoption of rules of responsible behavior and codes international standards of good conduct to prevent conflict situations in the cyberspace, ensuring strategic stability and, where appropriate, in the long term, serving as a reference to possible developments in international law.

DEVELOPING A SHARED LIO CULTURE: Effects to be integrated in a coalition

France is a major player in NATO and European partnerships in the cyber field.

Cooperation in cyberspace is not self-evident and is part of a complex logic. In the face of the cyber threat, the disparities in partners' capacities, organization, doctrines and investments are an additional challenge. That is why, in 2016, within the framework of NATO, France and its allies signed a commitment inviting member countries to acquire cyber resources to ensure their individual and collective security: The Cyber Defense Pledge.

In line with this commitment, France has committed itself, as its main partners, to partners, to share the effects produced by its own means of LIO for the purpose of defense or collective military operations, but always with control and control over the national control because they fall under our strict sovereignty.

At the European level, France is a driving force in the promotion of a culture military cyber-shared and aims to develop the means of interoperability with our main European partners.

France's international commitments in the cyber field, illustrated by the signature of MoUs or technical approvals governing cooperation, testify to the willingness to build a cyber defense policy with international partners on the entire spectrum (LID and LIO); a prerequisite for defense today of our strategic interests.

FACING A CHALLENGE FOR THE FUTURE: the LIO, a military employment capability to be developed

The development of offensive computer warfare capabilities for the benefit of the armed forces is entrusted to the General Directorate of Armaments (DGA), as with any other military capability. Due to the sensitivity and dynamics of the field, COMCYBER teams and DGA cyber teams are working closely together to develop and implement a capability Road Map.

The LIO must continue its development around five main challenges:

- **accelerate the production of offensive IT tools** for the benefit of the armed;
- **define an HR policy** that will make it possible to meet the expertise challenges of this new capacity;
- **initiate training actions** for the employment of the LIO for military purposes, within staffs for planning and conducting joint operations;
- **adapt our capacity acquisition and development processes** to the dynamics and speed of innovation in the cyber world;
- **converge with partners, particularly European partners, on ambitions operational** to enable us to act in coalition including with the LIO on a place of crisis.