Denys Kolesnyk

France Unveils Information Operations Doctrine

◁ *France already takes cyber defence seriously, but the new L2I law should be seen as covering complementary activities, not competing ones. (Image: French government)*

At a press conference in late October, France's Minister of Defence, Florence Parly, and Chief of the General Staff, Gen Thierry Burkhard, unveiled the Military Doctrine for Information Warfare *(Doctrine militaire de lutte informatique d'influence – L2I)*, adding another important piece to the doctrinal development in recent years regarding cyber and information warfare capabilities.

Moscow rushed to denounce France through the lips of Russia's Foreign Ministry spokeswoman, Maria Zakharova, for turning *"the information space into a field of combat so openly,"* and accused Paris of *"almost officially adopting a course on the militarization of social networks, on the transformation of the auxiliary tools of 'classic' military propaganda, into an independent type of weapon"*.

Such reaction from Russia is to be expected, but the accusations are groundless, given the role Moscow has adopted in information warfare activities for at least a decade. It is also worth bearing in mind that Russia has itself pioneered the application of information warfare components and tactics in the most advanced manner, on numerous occasions.

In 2020, Facebook removed several networks of fake accounts linked to Russia and France, and accused them of conducting *"interference campaigns"* in Africa. The joint report published the same year by ***Stanford Internet Observatory*** and ***Graphika***, explained that France merely reacted to Russian operations, especially in Mali. This may be the first publicly revealed information operations clash between Moscow and Paris, or in a foreign information space.

Given this context, we can assume that by unveiling the *"public elements"* of the L2I, France officially enters the information warfare playground, where such powers as Russia, China and some other minor states have already been active for quite some time. Although there are important differences that distinguish a democracy from authoritarian states, for instance by excluding national territory from activities covered by L2I, as well as voluntarily imposing certain limitations. Minister Parly announced, for example, that *"French forces will not destabilise a foreign state through actions that would, for instance, targets the electoral process"*.

The understanding of 'information operations' or, rather 'military influence operations' *(opérations militaires d'influence – OMI)*, is not something new for France; the concept was first raised in the 2000s. The L2I doctrine explains the new term 'Cyber Influence Warfare,' which significantly exceeds OMI. The L2I should be understood as *"military operations conducted in the information layer of cyberspace to detect, characterise and counter-attack, support StratCom, provide information (intelligence) or deceit, as a standalone operation or in combination with other operations"*.

In other words, this definition is braoder than the cyber domain or information operations in their most basic forms, exceeding the limitations of providing information support for 'boots on the ground'. It also reminds us of the Russian predilection for 'information confrontation', albeit without conducting operations domestically, and excluding the possibility of interference with the electoral process overseas.

The L2I doctrine acknowledges that information warfare is already a *"daily reality"* for the French armed forces, and describes the objectives and types of operations. For instance, among L2I military objectives, there are: *"detect and characterise enemy information attacks [or] weaken the legitimacy of our adversaries"*. As for L2I types of military operations, the document notes the activities to *"mislead the adversary to make him reveal his intentions; […] promote the activities of the armed forces on social media [or] denounce the inconsistencies or lies of the adversary"*.

An inescapable element of this doctrine is respect for the domestic legal framework and international law. The authors made a separate chapter explaining that, in peacetime, the L2I military operations *"respect the United Nations Charter and the principle of non-interference,"* and that they fall within the *"legal framework applicable to the engagement of the armed forces"*. Even during an armed conflict, they respect the rules of international humanitarian law.

The document also outlines the financial and other resources to implement the doctrine. For instance, the Military Programming Law (effectively the defence budget authorisation) for 2019-2025 allocates significant resources to cyber defence, allowing the MoD to increase by 770 additional personnel the initial objective of recruiting 1100 'cyber warriors,' while around €1.7 billion is expected to be allocated to the needs of cyber defence: a portion of those funds will be authorised for L2I activities.

From the publicly available information, it seems that this document has a non-ezxclusive but pronounced focus on conducting L2I activities where French troops are present or about to be deployed – effectively, mainly in the African theatre. The doctrine also allows for official attribution of enemy information operations, unlike cyberattacks, for which Paris prefers the non-attribution approach.

L2I activities should not be confused with cyber operations, or other initiatives such as those of the recently-created Viginum, an agency that focuses on analysing and countering disinformation coming from abroad, aimed at destabilising the French state.

Resident in Paris, ***Denys Kolesnyk*** *specialises in information warfare, cyber and wider European defence issues.*