France bolsters cyber capabilities and commitment through new doctrine

[Content preview – Subscribe to **Jane's Intelligence Review** for full article]

France unveiled its first offensive cyber doctrine in January 2019, joining other Western states that are avowing a readiness to strike in cyberspace. *William Moray* surveys the doctrine's likely effects and its differences from the Anglosphere approach

Key Points

- France launched a new offensive military cyber doctrine in January that marks a milestone and provides some insight into how the country conducts offensive cyber operations.
- The doctrine does not explicitly aim to deter hostile cyber activity, but it sends clear messaging to potential cyber attackers and marks a shift towards partial public attribution of some cyber attacks.
- France's commitment to offensive and defensive cyber capabilities will rise in the next spending cycle through to 2025, with increased recruitment, expenditure, and capabilities.

On 18 January 2019, French Minister of the Armed Forces Florence Parly and Chief of the Defence Staff (Chef d'État-Major des Armées: CEMA) General François Lecointre held a press conference in Paris. They unveiled France's first offensive military cyber-operations doctrine and made excerpts available to the public. The document, entitled 'Public Elements of the Offensive Cyber Military Doctrine', details how the country uses offensive cyber tools at an operational and tactical level, explaining the interaction with conventional forces and highlighting the circumstances under which the armed forces would conduct offensive cyber operations.

France recognised the importance of cyber defence as part of its security policy in the late 2000s. Several official documents made references to this effect, acknowledging that it had been included in the national defence strategy. The first occurrence was the 2008 White Paper on Defence and National Security, which included a brief mention of offensive cyber operations, among five references to cyber security.

The 2013 White Paper and the 2017 Defence and National Security Strategic Review had a substantially higher number of references to cyber and specifically mentioned the "offensive capabilities" of the country. Crucially, then-minister of defence Jean-Yves Le Drian announced the future creation of a cyber command during a pioneering speech in Bruz, Brittany, in December 2016. Le Drian stated that in certain circumstances, a cyber

attack could constitute an act of war; he also mentioned offensive cyber capabilities on many occasions and called for the drafting of a military doctrine.

Following Le Drian's speech, the Cyber Defence Command (COMCYBER) was established in January 2017 and placed under the direct authority of the CEMA. Finally, a Strategic Review of Cyber Defence document was published in 2018 to establish the principles of cyber defence in France.

French Minister of the Armed Forces Florence Parly delivers a speech on the military's cyber-defence strategy in Paris on 18 January 2019. During the speech, she revealed elements of France's first offensive cyber doctrine. (Thomas Samson/AFP/Getty Images) 1734905

The 2019 doctrine marks a crucial milestone. Only excerpts have been made available to the public; for security reasons, these public elements exclude information about France's operational cyber capabilities. Nevertheless, the published sections of the doctrine provide some insight into how France conducts offensive cyber operations.

Arthur Laudrain, a doctoral researcher in cyber security at the University of Oxford, told *Jane's* on 15 February 2019 that the doctrine "completed the [2018] Cyber Strategic Review", as the review focused on the strategic level. Laudrain added, "It translates into operational guidelines the strategic principles which were established by the [2018] Review."

French model

The rise of the French cyber-security culture and various organisational and institutional initiatives have resulted in the creation of a cyber-defence model that is substantially different from its UK or US counterparts. Those differences range from the organisational guidelines of cyber defence to the operational use of cyber tools, including offensive cyber strategies.

The first characteristic is at the organisational level. France's cyber model implies a strict partition between agencies with offensive capabilities and their defensive agency counterparts. Furthermore, according to this system, a distinction must be made between means of 'cyber protection' and capabilities that are dedicated to intelligence and the conduct of offensive operations.

As stated in the 2018 Strategic Review of Cyber Defence, this model is different from the Anglosphere's models, in which the "cyber defence capabilities are concentrated in the intelligence community", more specifically with the intelligence agencies specialised in signals intelligence (SIGINT), such as the US National Security Agency (NSA) or the UK Government Communications Headquarters (GCHQ) through its National Cyber Security Centre (NCSC).

The key factor that drives this organisational choice is the assumption that the state is best equipped to protect individual liberties, such as privacy. Therefore, the French model aims to encourage better co-operation between state-led agencies in charge of cyber protection and private entities. In its preamble, the offensive cyber doctrine confirms this separation between offensive and defensive cyber capabilities.

The second characteristic concerns the entities in charge of offensive cyber operations. Before the 2019 doctrine, offensive cyber operations were the prerogative of the French foreign intelligence agency, the Directorate-General for External Security (Direction Générale de la Sécurité Extérieure: DGSE), because of the clandestine nature of such operations. The 2013 White Paper was specific about this. Laudrain told *Jane's* that under the new doctrine, offensive cyber capabilities will be "co-ordinated by the COMCYBER, bringing together chiefs of staff, special operations, and foreign intelligence under a single operational chain", called the 'military-action' chain.

The 2018 Strategic Review of Cyber Defence called for the establishment of four operational chains, each with a specific focus: protection, intelligence, legal investigation, and military action. The objective of these operational chains is to improve the co-ordination of the organisations engaged in cyber operations, depending on their role and focus. The 2019 doctrine also highlights that offensive cyber capabilities are under the jurisdiction of the military-action chain.

Supporting conventional forces

The third characteristic occurs at the operational and tactical levels and is therefore particularly important in the offensive cyber doctrine. The doctrine establishes that France

prefers to use offensive cyber capabilities not as an independent tool, but rather in support of conventional forces, meaning that the chosen model is one of combined effects with conventional forces.

[Continued in full version…]

(839 of 3083 words)

For the full version and more content: