The French cyber defence strategy

BRENNUS 4.0

Madame Aude Géry [1] , chercheur associé au sein de GEODE

Published on 27/03/2020

Sciences & technologies

The expansion and interconnection of information and communication systems have created new challenges for States, both in terms of development and security. To face these challenges, States, including France, have adopted different strategies, depending on their history and functioning, but also on the way cyberspace has been approached [2]. The French cyber defence strategy is characterized by several doctrinal and organizational characteristics that are specific to it. While the last two years have been particularly prolific at the doctrinal level, there has been continuity and coherence of action aimed at providing France with the means to ensure its security, and that of its citizens, in cyberspace, but also to project its power into it.

The expansion and interconnection of information and communication systems have created new challenges for States, both in terms of development and security. To face these challenges, States, including France, have adopted different strategies, depending on their history and functioning, but also on the way cyberspace has been approached [2]. The French cyber defence strategy is characterized by several doctrinal and organizational characteristics that are specific to it. While the last two years have been particularly prolific at the doctrinal level, there has been continuity and coherence of action aimed at providing France with the means to ensure its security, and that of its citizens, in cyberspace, but also to project its power into it.

France's cyber defence strategy: the choice of a global approach

"At a time when computer attacks are likely to seriously harm the nation's interests at any time, our country must adapt its cyber defence posture with the ambition of better enforcing its digital sovereignty" [3]. It is with these words that the Cyber Defence Strategic Review, presented on 12 February 2018, introduces the French cyber defence strategy. It thus endorses a change of approach that began with the publication of the National Strategy for Digital Security in 2015 [4] . Until 2015, France adopted a technical-

military approach to cybersecurity, i.e. based solely on the protection and resilience of information and communication systems. Since 2015, it has adopted a global approach, i.e. based on digital security, which has penetrated all economic and societal fields.

A global approach based on an organizational model dominated by ANSSI and characterized by the separation of offensive and defensive missions.

In order to ensure its digital sovereignty, since the 2008 White Paper on Defence and National Security, the first strategic document to mention cyberspace as a strategic space, France has continued to strengthen its organizational, capacity, human and legal resources to ensure its cyber defence. Succeeding the Central Directorate of Information Systems Security, the National Agency for Information Systems Security (ANSIS), which was created in 2007, has been responsible for(ANSSI) was created in 2009[5] and designated as the national authority in charge of information systems security in 2013[6]. 6] Placed under the authority of the Prime Minister, it is the cornerstone of the organisation of French cyber defence. Charged with the coordination of the French cyber defence strategy, its missions have been progressively extended by the military programming laws of 2013[7] and 2018[8]. It is thus in charge of the defence and security of the State's information systems. In addition, it has regulatory power to set the rules that must be implemented by vital operators to protect their information systems.In addition, it has regulatory power to lay down the rules to be implemented by vitally important operators to protect their vital information systems, the power to certify and qualify products and services, and finally the power, in the event of a major crisis, to impose measures on these operators. The broadening of its missions and the approach adopted by the 2015 Strategy, and then the Cyber Defence Strategic Review, will require the The broadening of its missions and the approach adopted by the 2015 Strategy and the Strategic Review of Cyber Defence will require the involvement of other actors, such as the Ministry of the Interior, the Ministry of Justice or the Ministry of Europe and Foreign Affairs. The result is a profoundly inter-ministerial strategy, which is reflected in the operational chains and governance of cyber defence, created and modernised in 2018[9], coordinated by ANSSI.

What has characterized the French cyber defence strategy since its inception is its model of organization and governance. It is based on a fundamental principle: the separation of offensive (intelligence and offensive operations) and defensive (network protection and defence) missions and capabilities, thus distinguishing it from Anglo-Saxon models[10]. 10] This separation aims to "guarantee better coordination between the ANSSI and military cyber defence" and to "facilitate a work of trust between the ANSSI and companies" [11]. 11] The ANSSI thus does not have the power to conduct offensive operations. This separation does, however, contain ambiguities. Indeed, the ANSSI, in order to respond to a computer attack affecting the Nation's security, can "carry out the technical operations necessary to characterise the attack and neutralise its effects by accessing the information systems that are at the origin of the attack" [12]. [12] However, insofar as they consist in penetrating third party systems without the authorization of the owner or administrator, these technical operations can be qualified as offensive operations. However, this model, confirmed in the Strategic Cyber Defence Review, offers many advantages that can strengthen the nation's resilience to cyber threats.

A global approach aimed at ensuring France's digital sovereignty

The Cyber Defence Strategic Review is clear: "[f]or France's cyber defence, beyond that of the State itself and vital operators, the overall level of cybersecurity in society must be raised. To be effective, it is indeed a matter of envisaging, in a logic of digital sovereignty, a cyber defence in the depths of our country integrating that of citizens, businesses and local authorities" [13].

However, it contains a semantic ambiguity linked to the concept of digital sovereignty. Indeed, digital sovereignty is defined as " France's capacity to act in a sovereign manner in the digital space, while maintaining an autonomous capacity to apprehend and manage the digital environment" [14]. ciation, decision and action, on the one hand, and on the other hand, to preserve the most traditional components of its sovereignty against new threats that take advantage of the increasing digitization of society" [14]. It is therefore understandable that the concept of digital sovereignty refers to that of digital strategic autonomy. As Alix Desforges notes, this echoes "a concept closely linked to the notion of decision-making autonomy developed by the nuclear deterrence theorist General Poirier" [15]. [15] Autonomy of decision is the ability to identify and characterize threats in order to be able to respond to them. It presupposes prior identification of sovereign activities and requires the availability of clean technologies to carry them out. Drawing the consequences of this objective, the Strategic Review of Cyber Defence then identifies technologies whose mastery is essential to the exercise of this decision-making autonomy: encryption of communications, detection of computer attacks, professional mobile radios, the cloud and artificial intelligence [16].

This semantic confusion does not, however, completely overshadow the traditional aspects of sovereignty. As a State, France is by nature sovereign and therefore exercises its prerogatives in the digital space. While this exercise may be made difficult by the cross-border nature of the networks and the multiplication of conflicts of jurisdiction, the very principle of its sovereignty cannot be called into question. Furthermore, digital strategic autonomy, which is a watermark of digital sovereignty, contributes to the exercise of that sovereignty by aiming to provide France with the means to exercise its powers, and in particular to apply its national law, on its territory and its citizens.

The place of the Armed Forces in the French cyber defence organisation

The French cyber defence strategy cannot be presented without mentioning the particular role and place of the Ministry of the Armed Forces in the French cyber defence model. In 2008, cyberspace was identified in the White Paper on Defence and National Security as "a new field of action in which military operations are already taking place" [17]. 17] It is this representation of cyberspace as a field of confrontation that will give the Ministry of the Armed Forces a special place in the French cyberdefense system. The appointment of a General Cyber Defence Officer, attached to the Deputy Chief of Operations of the Armed Forces Staff in 2011 will then mark the beginning of the rise of the Armed Forces in this field. Indeed, if the ANSSI is the national authority in charge of defence and the security of information systems, what has since become COMCYBER has a special place: it is in charge of network security for the Ministry of the Armed Forces as well as the conduct of military operations in cyberspace. The military programming law of 2013 marks a change of scale by organising a real operational cyber defence chain. The evolution will continue with the creation, in 2017, of the Cyber Defence Command (COMCYBER), which will be placed directly under the authority of the Chief of Defence Staff, and the presentation of the Cyber Strategy for the Armed Forces on 18 January

2019.

Presented by Florence Parly, Minister of the Armed Forces, and by General Lecointre, Chief of the Armed Forces Staff, the Cyber Army Strategy is the first strategic document of the Armed Forces dealing exclusively with cyber defence, some elements of which have been made public. Indeed, two documents, the Public Elements of Military Offensive Cyber Warfare Doctrine and the Departmental Defensive Cyber Warfare Policy, were published following the Minister's speech[19]. [19] While they have been particularly noteworthy because of elements dealing with offensive cyber warfare, it should be noted that they do not in any way constitute a break in the French military cyber defence strategy. On the contrary, they are in line with the Revue de la défense et de la sécurité nationale and the Revue stratégique de cyberdéfense by aiming to provide the Armed Forces with es with a strategy enabling them to ensure their superiority in this space and thus ensure the Nation's security and fully exercise its sovereignty. Moreover, the fact that they assume responsibility for developing, holding and using offensive capabilities is nothing new. Indeed, as early as 2008, the White Paper recognized the need for France to acquire such capabilities[20]. 20] These two documents nevertheless mark an important step in the construction of the French military cyber defence strategy, not only by organizing a standardization of the offensive, but also by participating in the strengthening of the cyber power posture that France intends to take advantage of[21].

21] France's proactive international cyber defence strategy

The final key element of France's cyber defence strategy concerns its international strategy. Although the appointment of the first ambassador in charge of cyber defence issues only dates from 2014, France has participated in all rounds of United Nations negotiations on information and communication technologies in the context of national security since 2004. It has also played an active role in the drafting of the Convention on Cybercrime, adopted by the Council of Europe in 2001, and has, in particular, been a party to the Convention on Cybercrime.s Wassenaar Arrangement for the listing of intrusion software on the List of Dual-Use Goods and Technologies. The appointment of a digital ambassador with an extremely broad mandate in 2017, followed a few weeks later by the publication of France's International Digital Strategy, entered into force on 1 January 2007.rmed the key role of the Ministry of Europe and Foreign Affairs in the development and implementation of France's cyber defence strategy. They also marked France's choice to be a leading player in the international security and stability of cyberspace.

The Strategic Cyber Defence Review thus devotes lengthy sections to France's objectives by proposing to go further in the development of the international legal framework, through the promotion of standards of responsible behaviour by States. In addition, it details, for the first time, its vision of the application of international law in cyberspace[22]. 22] Finally, it proposes new rules and standards concerning the responsibility of non-state actors for the use of offensive tools and the responsibility of corporations for the design and maintenance of digital products. The launch of theParis Appeal for Security and Stability in Cyberspace[23], with the extremely activesupport of Microsoft[24], in November 2018, is France's latest international initiative. Signed by more than 60 States and 500 non-state actors, this document lists political commitments, some of them new, aimed at strengthening the security and stability of cyberspace. Marked by its multi-actor character, it is in line with the recognition of the shared but differentiated responsibilities of all actors, whether they are States, non-State actors, or non-State actors.s support for

the Global Commission on the Stability of Cyberspace, to make progress in this area.

However, France's international strategy must not be limited to issues of international peace and security and Internet governance. Indeed, France's diplomatic activity is also represented by technical cooperation in the field of cybersecurity, mainly led by ANSSI, or cooperation in the military field implemented by COMCYBER, notably in the framework of NATO. All these initiatives thus contribute to the projection of France's digital power and constitute an important pillar of its strategy.

France's cyber defence strategy is characterised by its comprehensive approach, both in terms of content and actors. It aims to enable France to ensure its security and that of its citizens and to project its power into cyberspace. Aymeric Bonnemaison and Stéphane Dossé wrote in 2014 that "it [therefore] seems necessary for States to 'plant the flag'" [25] in cyberspace. From this point of view, France has certainly begun to do so by devoting significant efforts to the rise of French cyber defence, both defensively and offensively. At the same time, its action is characterized by a desire to advance the security and stability of cyberspace by participating actively in international negotiations in this area, and by promoting greater responsibility on the part of all the actors concerned. Finally, at both national and international level, its action is based on the principle of cooperation, which is a prerequisite for ensuring its security in cyberspace and the stability of the global information environment.

———————

1] Aude Géry is a doctoral student in public international law at the University of Rouen. Her thesis is on the proliferation of digital weapons. She is also an associate researcher at GEODE, a research and training centre on the geopolitics of the Datasphere, and a reserve officer at the EMSST.

2] Frédérick Douzet (dir.), Cyberespace : geopolitical stakes, Hérodote, n°152-153, 1st-2nd quarter 2014, 313 p.

3] Revue stratégique de cyberdéfense, 2018, p. 7.

4] For an analysis of the evolution of the French cyber defence strategy, see Alix Desforges, Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France, Thesis, Université Paris 8, 2018, 395 p.

5] Decree No. 2009-834 of 7 July 2009 creating a service with national competence called the "National Agency for the Security of Information Systems".

6] Law n°2013-1168 of 18 December 2013 relating to military programming for the years 2014 to 2019 and containing various provisions concerning defence and national security, article 21.

7] Ibid. Articles 21 and 22.

8] Law n°2018-607 of 13 July 2018 relating to military programming for the years 2019 to 2025 and containing various provisions relating to defence, Article 34.

9] Strategic Cyber Defence Review, op. cit. op. cit., pp. 52-55.

10] For example, in the United Kingdom, the Government Communication Headquarters (GCHQ), a technical intelligence service, is responsible for offensive operations and the state's cyber security and cyber defence. The National Cyber Security Centre, responsible for the protection of computer systems, is a division of the GCHQ.

11] Danilo D'Elia, La cybersécurité des opérateurs d'importance vitale: analyse géopolitique des enjeux et des rivalités de la coopération public-privé , Thesis, University of Paris 8, 2017, pp. 116-117.

12] Law n°2013-1168 of 18 December 2013 relating to military programming for the years 2014 to 2019 and containing various provisions concerning defence and national security, article 21.

13] Revue stratégique de cyberdéfense, op. cit. , p. 93.

14] Ibid.

15] Amaëlle Guiton, "Internet: des États entre 'souveraineté numérique' et 'autonomie stratégique,' Libération, 13 February 2019, available at https://www.liberation.fr/planete/2019/02/13/internet-des-etats-entre-souverainete-numerique-et-autonomie-strategique_1709212.

16] Ibid at 96 et seq.

17] Livre Blanc de la défense et de la sécurité nationale, 2008, p. 53.

18] Alix Desforges, Approche géopolitique du cyberespace, enjeux pour la défense et la sécurité nationale, l'exemple de la France, op. cit. , p. 120-156.

19] Here again, we note the choice to separate the offensive missions from the defensive missions, even if, as the Public Elements assert, the offensive computer warfare can be put at the service of the defensive computer warfare.

20] White Paper on Defence and National Security, op. cit. , p. 53.

21] For an analysis of these documents, see François Delerue, Alix Desforges, Aude Géry, "A Close Look at France's New Military Cyber Strategy," War on the Rocks, 23 April 2019, available at https://warontherocks.com/2019/04/a-close-look-at-frances-new-military-cyber-strategy/; Stéphane Taillat, "Signaling, Victory, and Strategy in France's Military Cyber Doctrine", War on the Rocks, 8 May 2019, available at https://warontherocks.com/2019/05/signaling-victory-and-strategy-in-frances-military-cyber-doctrine/.

22] François Delerue, Aude Géry, "France's Cyberdefense Strategic Review and International Law," Lawfare, 23 March 2018, available at https://www.lawfareblog.com/frances-cyberdefense-strategic-review-and-international-law.

23] https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la.

24] Martin Untersinger, "La France veut relancer les négociations sur la paix dans le cyberespace," Le Monde, 8 November 2018, available at https://www.lemonde.fr/pixels/article/2018/11/08/la-france-veut-relancer-les-negociations-sur-la-paix-dans-le-cyberespace_5380571_4408996.html.

25] Aymeric Bonnemaison, Stéphane Dossé, Attention: Cyber! Vers le combat cyber-électronique, Economica, 2014, p. 79.

Title : Madame Aude Géry [1] , chercheur associé au sein de GEODE

Author (s) : Madame Aude Géry [1] , chercheur associé au sein de GEODE

Release date 18/03/2020

FIND OUT MORE