



CRITICAL TECHNOLOGIES AND INDUSTRIAL CAPABILITIES: NATIONAL DEFINITION AND POLICY IMPLICATIONS

The French case

Alice Pannier / Research Fellow, Head of Ifri's
Geopolitics of Technology Program

September 2022



ABOUT THE AUTHOR



Alice Pannier / Research Fellow, Head of Ifri's Geopolitics of Technology Program

Alice Pannier heads the Geopolitics of Technology program, launched at Ifri in October 2020, after having been associate researcher since 2019. Her research focuses on the geopolitical dimension of new technology, European technology policies, and transatlantic relations. She has also worked for a long time on European security and the foreign and defense policies of European countries, especially France and the United Kingdom.



The Armament Industry European Research Group (Ares Group) was created in 2016 by The French Institute for International and Strategic Affairs (IRIS), who coordinates the Group. The aim of the Ares Group, a high-level network of security and defence specialists across Europe, is to provide a forum to the European armament community, bringing together top defence industrial policy specialists, to encourage fresh strategic thinking in the field, develop innovative policy proposals and conduct studies for public and private actors.

CONTACT [PILOTS]

Jean-Pierre Maulny, Federico Santopinto, Olivier de France, Sylvie Matelly
ares@iris-france.org
+33 (0)1 53 27 60 60

iris-france.org/ares
#ARESGroup



@AresGroup_EU



ARES Group - EU

ABSTRACT

France has historically paid significant attention to strategic technologies and industries, whether they were strictly defence- and nuclear deterrence related, or considered as vectors of national independence and security, more broadly. This has translated into policies aimed at supporting the national industrial and technological base, funding R&D, and protecting strategic companies from foreign takeovers. In recent years, the notion of “critical technologies” was adopted, and the breadth of sectors covered by national strategies and investment plans has expanded to include emerging and green technologies. That being said, in many areas of digital technologies, such as cloud computing, the French government continues to rely largely on foreign (in particular, non-European) providers. Finally, the French policy has been increasingly intertwined with the EU level, as France has been a key promoter of initiatives to enhance the EU’s role and clout in critical and emerging technologies, in defence as well as in the civilian domain.

Keywords: France / Critical Technology / Defence Industrial Policy / European Union / Foreign Direct Investments regulation / Innovation

DEFINITIONS OF CRITICAL TECHNOLOGIES AND INDUSTRIES IN FRANCE

There are several ways critical technologies and industries are defined at the French national level. At the broadest level, the “essential interests” of France cover matters of public order, public health, public security, and national defence, in accordance with European treaties¹. Technologies and industries that contribute to upholding those interests may thus potentially be considered critical. More precisely, the Covid-19 pandemic led to a new reflection on the “vital” functions of the State to ensure the country’s continuation, to include: the provision of health, food, water, energy, and telecommunications². To that were added “strategic” domains and technologies that contribute to the green transition and to “digital sovereignty”.

France implements a screening mechanism for foreign direct investments (FDI) in critical technological sectors. While in France, the FDI mechanism largely pre-dated the EU’s 2019 regulation on the matter (it was first established in 1966, and reinforced in 1996), the notion of “critical technologies” was adopted as part of the EU framework³. The “critical technologies” mentioned in French law as of December 2019 were: cybersecurity; artificial intelligence; robotics; additive manufacturing (i.e., 3D printing); semiconductors; quantum technologies; and energy storage.⁴ The list was extended in January 2022 to include biotechnology and the technologies involved in the production of renewable energy⁵. These come in addition to defence activities, military technology, cryptography, dual-use items, and other strategic technologies that are already subject to specific legal regimes.

Another way of framing critical sectors is through the list of sensitive *activities* that are subject to FDI screening (see below), which also include: “Data processing, transmission or storage activities the compromise or disclosure of which is likely to prejudice the exercise of sensitive activities”, and “the operation of electronic communications networks and services”⁶.

¹ Plan d’Action Pour la Croissance et la Transformation des Entreprises (« PACTE »), September 2019, p.58.

² Commissariat au Plan, “Produits vitaux et secteurs stratégiques : comment garantir notre indépendance ?”, December 21, 2020, available at: www.gouvernement.fr.

³ Loi n° 66-1008 du 28 décembre 1966 relative aux relations financières avec l'étranger. <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000880207/2022-05-26>

⁴ 1° of III of article R. 151-3 of the Monetary and Financial Code of December 2019

⁵ Direction Générale du Trésor, « Les secteurs d'activités dans lesquels les investissements sont soumis à autorisation préalable », published 25 November, 2021, available at www.tresor.economie.gouv.fr.

⁶ Ibid.

MONITORING DEPENDENCIES LINKED TO CRITICAL TECHNOLOGIES AND INDUSTRIES

Historically (since the beginning of the 5th Republic), the defence and technological industrial base (DTIB) has been seen in France as a cornerstone of national strategic autonomy, with, at its heart, the independent nuclear deterrent. As a result, there is a long tradition in France of monitoring strategic industry, and seeking to preserve national design and manufacturing capacity in a wide range of defence technologies (complex weapons, ships, aircraft, land vehicles...) but also key enabling technologies (satellites, microelectronics, computing, telecommunications). Companies in these sectors are thus closely monitored. For defence companies, the interministerial service General Secretariat for National Security and Defence (SGDSN) and the Directorate General for Armament (DGA) have responsibility in protecting the Defence Industrial and Technological Base (DTIB) from foreign influence. Typically, the DGA's Service for industrial affairs and economic intelligence works alongside the Ministry for the Economy to check that foreign investors will respect certain conditions to preserve a company's France-based factories and know-how⁷.

Aside from the DTIB, as a result of its historical law on FDI, the French State is relatively well armed to monitor risks of dependencies stemming from foreign takeovers of French strategic companies. The state monitors and can block foreign investments to a greater extent than what the EU's FDI screening mechanism provides for. The PACTE law⁸, adopted in 2019, strengthened the examination procedure for FDI, and broadened the state's power to gain some control over companies through special shareholding. In addition, there has been an active use of State equity investments in certain companies and by the intervention of public authorities to support or counter certain merger-acquisition operations.⁹

Recent updates to the PACTE law have extended the sectors that fall under state supervision (see the list above), and lowered the threshold of foreign (i.e., non-EU or EEA) ownership from 25% to 10%. In application of that law, in 2020, the French government blocked the proposed acquisition of Photonis, which provides military night-vision equipment to the French armed forces, by the American company Teledyne. In January 2021, the French Ministry of Finance blocked the acquisition of Carrefour by the Canadian Couche-Tard, which was justified out of

⁷ H. Meddah, "Comment la DGA protège les entreprises stratégiques françaises", L'Usine Nouvelle, 26 October 2020, available from www.usinenouvelle.com.

⁸ PACTE : « Plan d'action pour la croissance et la transformation des entreprises », which means Action plan for business growth and transformation.

⁹ France Stratégie, *Les politiques industrielles en France : Évolutions et comparaisons internationales*, November 2020.

“food sovereignty” concerns. These two examples indicate a broad conception of sovereignty in France, and a willingness to block acquisitions even when they come from Allied countries.

Finally, when it comes to procuring from foreign providers for critical infrastructure (digital services and hardware), the security risks foreign providers of can pose have also become the object of greater scrutiny. For instance, just like in many other democracies, 5G networks and infrastructure have also been subject to review. In 2020, the information system security agency, ANSSI, decided that licences to deploy Huawei equipment would be authorised only for a limited period, which effectively amounts to phasing out Huawei 5G equipment from French territory by 2028.¹⁰ Besides, in the case of cloud infrastructure, the decision to have Microsoft host the planned “Health Data Hub” – supposed to centralise the medical data of French citizens for research purposes or research – was debated due to concerns over the level of legal protection that could be guaranteed for that sensitive data.¹¹ A decision was made to reverse this choice and opt for a “sovereign” alternative, but its implementation was postponed until 2025, due to a lack of a viable national alternative¹². A similar decision has been under consideration regarding the French domestic intelligence service, DGSI, and its contract with the American software company Palantir which provides it with big data analytics tools. However, the dependency on Palantir has remained, for the same reason¹³.

ADDRESSING POTENTIAL OR CONFIRMED DEPENDENCIES

As mentioned above, France has for decades led a defence policy that has resided in strong investment in research and technology, with the goal of avoiding the creation dependences on foreign technologies in the first place. In other words, an emphasis has been placed on having “sovereign” technological solutions: defence systems “that cannot be shared and where guarantees of hardware and software integrity, freedom of use, and operational superiority prevail”¹⁴. Despite a sometimes-tense financial situation over the past decades, defence has remained the third most important published budget, as well as the first source of public investment spending. Defence is still fuelling R&D and supports technology-intensive

¹⁰ Reuters, “Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028”, 22 July 2020.

¹¹ Alice Pannier, “The Changing Landscape of European Cloud Computing: Gaia-X, the French National Strategy, and EU Plans”, Briefings de l’Ifri, Ifri, 22 July 2021.

¹² L’Usine Digitale, “Microsoft restera l’hébergeur du Health Data Hub jusqu’en 2025 », 13 septembre 2022, <https://www.usine-digitale.fr/article/microsoft-restera-l-hebergeur-du-health-data-hub-jusqu-en-2025.N2043032>

¹³ « Le projet de big data des armées critiqué en commission défense », Lettre A, 29 October 2021.

¹⁴ Revue Stratégique, 2017, english version, p.65

sectors in both military and dual domain: the Ministry of Armed Forces remains the first public investor, with €6.6 billion in 2021¹⁵.

The 2017 Strategic Review of national defense and security suggested that emerging technologies a priori fall into the “sovereign” category¹⁶. Therefore, the Defence innovation agency (AID) was set up in 2018 to strengthen the link with French start-ups, harness the relevant dual innovations that take place in the civilian domain, and foster spin-in dynamics. Jointly with Bpifrance, it oversees €400 millions of dedicated investments. It has since, for instance, supported the quantum hardware start-up Pasqal in its early development stages. The satellite-based imagery intelligence company Preligens (ex-Earth Cube), founded in 2016, similarly has grown thanks to the financial support of the French ministry of Armed forces.

The past few years have also seen a strong focus on supporting innovation and R&D in critical sectors with a particular attention to start-ups beyond defence, in the civilian domain. This has led to a burgeoning of dedicated funds and investment plans. In 2019, the government set up an Innovation Council, co-chaired by the Minister for Higher Education and Research, and the Minister for the Economy, to coordinate and oversee the multiple streams of funding directed at innovation and disruptive technologies. These include the Innovation and Industry Fund, launched in January 2018, which endowed the public investment bank, Bpifrance, with €10 billion-worth of assets. About a third is dedicated to investing in deep tech start-ups in a bottom-up logic. The other two thirds are targeted to priority areas in a government-led top-down fashion (e.g., €100 million for AI, and €25 for nanoelectronics)¹⁷. Another stream of funding is the fourth Future Investments Program (PIA4), announced by the Prime Minister in September 2020 as part of the Covid-related stimulus package, and targeted toward academia and research. This includes a €12.5bn investment program over five years to “accelerate” innovation in certain sectors, with a particular focus on digital and clean technology, including AI, quantum, cybersecurity, 5G, clean hydrogen, digital health, and cloud computing.¹⁸ In October 2021, a new investment plan “France 2030”, worth €30 billion was announced, bringing additional support to several sectors, including space and transport.

¹⁵ Les chiffres clés de la défense, 2021

¹⁶ Ibid.

¹⁷ Plan d’Action Pour la Croissance et la Transformation des Entreprises, September 2019.

¹⁸ Gouvernement, “Stratégies d’accélération pour l’innovation”, last updated 10 December 2021, available at www.gouvernement.fr.

ARTICULATING NATIONAL POLICIES WITH THE EUROPEAN LEVEL

French technology policies fit well with European-level initiatives in recent years, which the French government has either supported or helped bring about. Such initiatives include the European Defence Fund (EDF), which was set-up officially in 2021, after two test programs. France and Germany, working alongside the EU Commission, were instrumental in the creation of the EDF — a program that encourages cross-border R&D in defence. Aside of defence-specific innovation, France has encouraged the setting-up of the European Innovation Council in 2017 (effective in 2021) to allow the EU to invest directly in SMEs and start-ups that conduct R&D in emerging technologies. Finally, France recently helped prop up a new initiative called Scale Up Europe, a venture capital fund which should eventually be endowed with €10 billion to support the growth of European digital start-ups. Bilateral cooperation in critical technologies is also developing, as illustrated with the France-Netherlands 2021 memorandum of understanding on quantum technologies, which preceded a merger between Pasqal and a Dutch quantum software start-up. Thus, government action at the national level has been fitting well with - and even building toward - the European level, as the latter is viewed as a key vehicle for reaching a critical mass necessary to compete at the global level.

The Armament Industry European Research Group



2 bis, rue Mercœur - 75011 PARIS / France

+ 33 (0) 1 53 27 60 60

ares@iris-france.org

iris-france.org/ares



The Armament Industry European Research Group (Ares Group) is a high-level network of security and defence specialists across Europe. Its aim is to provide a forum to the European armament community, bringing together top defence industrial policy specialists, to encourage fresh strategic thinking in the field, develop innovative policy proposals and conduct studies for public and private actors.