IFRI
MEMOS

Geopolitics of Technology Center |
Security Studies Center

ifri since 1979

FEBRUARY 16, 2026

Europe at the Deftech Crossroads

Rethinking the European Defense Innovation System

Alexandre PAPAEMMANUEL
Laure de ROUCY-ROCHEGONDE

Key Takeaways

- In the United States, DefTech is thriving thanks to unprecedented investments and the openly embraced financialization of the defense apparatus, enabling the large-scale militarization of civilian technologies (commercial space, cloud computing, AI).
- The Ukrainian theater is a testing ground for the wars of the future, where the line between hardware and software is increasingly blurred in favor of simple yet technologically impressive physical systems, enhanced by AI, whose operational use—now battle-tested—is bound to increase.
- A new operational model is thus emerging, based on the interplay between "decision-making weapons" and "attrition weapons," in a context where digital technology determines both effectiveness and resilience.
- The European response must therefore be to orchestrate this hybridization, ensuring that the robustness of large industrial groups and the agility of startups are compatible through explicit governance.

Introduction

"The way I look at Iron Dome is as the ultimate manifestation of the future of the United States' role in future conflicts, which is not to be the world police, but to be the world gun store,"[1] said Palmer Luckey in November 2023. Luckey is the founder of Anduril, one of the most prominent DefTech companies.[2] The ambition is clear: to participate in global rearmament by capitalizing on the quality of American innovations and to dominate the arms market—at least in the West—through technological mastery.

As operations increasingly rely on data and artificial intelligence (AI) and weapons systems become "software-defined,"[3] the advantage no longer lies solely in the design of platforms—fighter jets, tanks, submarines—but also in the mastery of information architecture—collection, fusion, computation (cloud/edge), interoperability—and in the ability to innovate very rapidly. War, in the age of AI, is therefore not solely the domain of states. It is an industrial and logistical matter, but also a financial one. In this post-Westphalian framework, sovereignty is expressed less in laws than in lines of code. Power is measured in APIs,[4] server latency, and the ability to fuse sensors and payloads.

The industrial partnership formed between Anduril and Palantir in December 2024 is emblematic of this shift.[5] These two companies, whose CEOs come from the tech sector and have no roots in the United States (U.S.) defense industrial and technological base, are now at the forefront of AI applications for national security, placing them at the heart of U.S. operational power. This agreement comes at a time when tech companies are attempting to capture a larger share of the colossal U.S. defense budget—estimated at $900 billion for 2026, and which Donald Trump aims to increase to $1.5 trillion by 2027—at the expense of traditional industry players such as Lockheed Martin, Raytheon, or Boeing.[6] Even more striking is that while the Anduril/Palantir consortium is open to "other industry players" such as SpaceX, OpenAI, or Scale AI, the "Primes" are not always invited.

1. "Palmer Luckey and Mike Solana on the Future of War, Israel, the TikTok Ban, & U.S. Manufacturing", *Pirate Wires Podcast*, November 10, 2023, available at: www.youtube.com.
2. DefTech plays a role in defense analogous to that of FinTech in finance and MedTech in healthcare: it injects a "product", software, and data-driven approach into a sector historically dominated by programs, long cycles, and significant regulatory constraints. This term refers to all companies—often born in the startup ecosystem—that develop technologies for military or security use (sometimes dual-use), combining software, data, AI, sensors, and hardware, with a focus on products suitable for industrial production and rapid deployment.
3. A system is said to be "software-defined" when its operation is controlled primarily by software rather than by fixed hardware.
4. "Application Programming Interface" or API.
5. Palantir Technologies and Anduril Industries—the former specializing in data analysis and the latter in autonomous systems—launched a consortium in early December 2024 to bid on Pentagon contracts. See Anduril's press release at: www.anduril.com.
6. T. Kinder and G. Hammond, "Palantir and Anduril Join Forces with Tech Groups to Bid for Pentagon Contracts", *Financial Times*, December 22, 2024, available at: www.ft.com.

Europe is experiencing a similar trend, driven by the rise of startups operating in the most advanced technology sectors.[7] As in the U.S., however, collaboration between these new entrants and established companies in the European defense industrial base remains complex. The terms of the relationship between these two worlds—agile innovation based on data on one side, established, equipment-focused structures on the other—remain largely undefined, and models for partnership, governance, and industrial integration have yet to be devised. How, then, can these forces be brought together to build a credible European capability in defense AI?

Lessons from Ukraine

This shift in the industrial landscape actually accompanies the strategic rupture observed in contemporary theaters of operations. Indeed, in Ukraine as in the Middle East, AI continues to permeate the battlefield. Its applications are as numerous as they are diverse: from observation and reconnaissance to autonomous weapon systems, including target identification and classification, threat analysis and prediction, logistics and resupply, cybersecurity, electronic warfare, simulation and training, military healthcare, and tactical decision support.[8]

In Ukraine as in the Middle East, AI continues to permeate the battlefield

The Russia-Ukraine conflict serves as a real-time innovation laboratory, where the conventional distinction between hardware and software is increasingly blurred, profoundly reshaping defense value chains.[9] The role of drones, often mass-produced and low-cost, attests to this shift: whether small first-person view (FPV) drones, long-range remotely operated munitions, or autonomous drones, these systems combine simple physical platforms with sophisticated software capabilities (AI, autonomous guidance, target recognition, computer vision, and signal networking) that maximize effectiveness relative to cost.[10]

Ukrainians purchased as many as 4.5 million FPVs in 2025,[11] for more than $2.6 billion—a rate of attrition akin to an ammunition economy. In the U.S., the rise of DefTech players and the awarding of contracts worth around $200 million to digital giants

7. C. Boutelet, “À Munich, les start-up du spatial et de la défense dessinent le futur de la tech européenne” [In Munich, space and defense startups are shaping the future of European tech], *Le Monde*, May 16, 2025, available at: www.lemonde.fr.
8. A. Férey and L. de Roucy-Rochegonde, “De l’Ukraine à Gaza : l’intelligence artificielle en guerre” [From Ukraine to Gaza: Artificial Intelligence in War], *Politique étrangère*, Vol. 89, No. 3, Ifri, Fall 2024.
9. G. Jones, J. Egan, and E. Rosenbach, “Advancing in Adversity: Ukraine’s Battlefield Technologies and Lessons for the U.S.”, *Policy Brief*, Belfer Center for Science and International Affairs/Harvard Kennedy School, July 31, 2023, available at: www.belfercenter.org.
10. K. Bondar, “Ukraine’s Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare”, Report, Center for Strategic and International Studies/Wadhwani AI Center, March 2025, available at: www.csis.org.
11. R. Rivaton, “Guerre en Ukraine : l’âge d’or des start-up de la défense” [War in Ukraine: The Golden Age of Defense Startups], *L’Express*, March 29, 2025, available at: www.lexpress.fr.

(OpenAI, xAI, Google, Anthropic) for the operational development of AI techniques[12] signal a transition toward a defense system conceived as an iterative, scalable software-industrial system.

In this new landscape, software serves as the strategic glue. It links hardware, sensors, intelligence flows, observation platforms, and operational decisions. The Delta system, deployed by Ukrainian forces to aggregate data from drones, satellites, radars, and ground units, is a compelling example. Within minutes, strikes can be targeted and tactical decisions implemented, significantly accelerating the detection, decision, and action loops.[13]

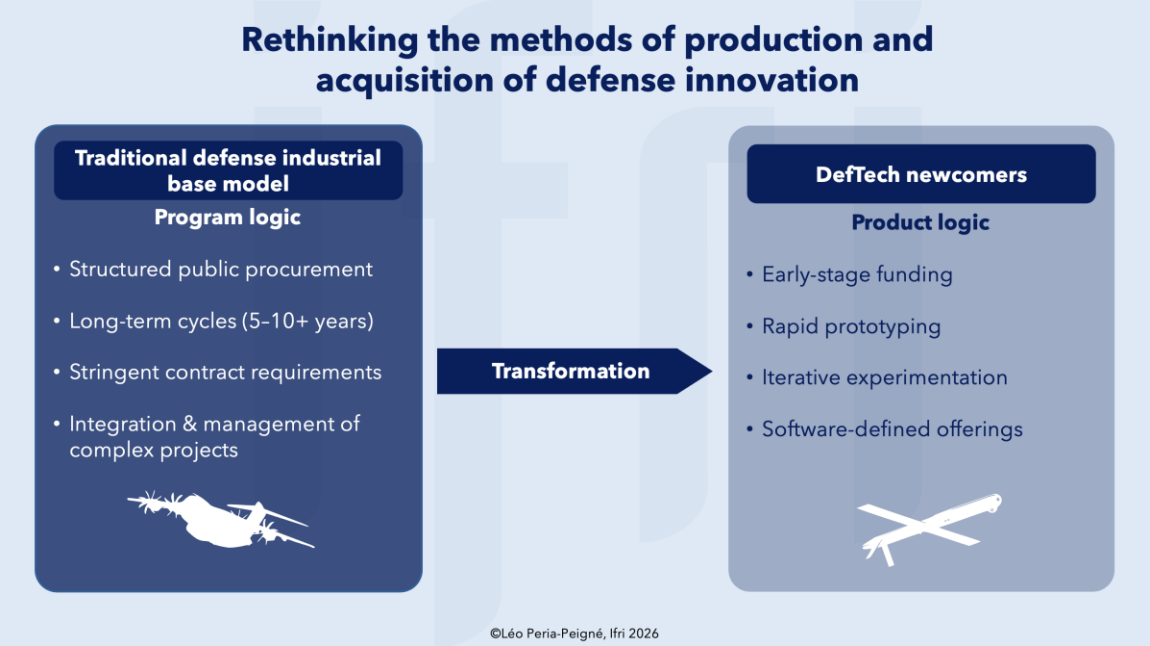
DefTech players finance, design, and deploy their innovations using their own funds

This is what leads Palmer Luckey to assert that "technology is now the greatest advantage on the battlefield"[14] or Alex Karp, CEO of Palantir, to state that "You only stop war by having the best technology and by scaring the bejabers—I'm trying to be nice here—out of our adversaries".[15] While the centrality of technological superiority in U.S. strategy is nothing new, these tech moguls no longer wait for institutional approval to expand the military arsenal. Unlike large firms driven by military demand—which rely on government tenders and contracts—DefTech players finance, design, and deploy their innovations using their own capital (or funds raised on the markets), guided by a vision rooted in algorithmic foresight, rapid decision-making, and the certainty that government contracts will follow.

From capital to sensors: A structural shift

The ongoing revolution lies not so much in the identity of the client—which remains the state—as in the reconfiguration of production and procurement methods. The traditional defense industry model is based on a program-driven approach, whereas, conversely, new entrants in DefTech favor a product-driven approach.

12. "US Defense Department Awards Contracts to Google, Musk's xAI", Reuters, July 14, 2025, available at: www.reuters.com.
13. G. Jones, J. Egan, and E. Rosenbach, "Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S.", *op. cit.*
14. P. Luckey, "Palmer Luckey: I Saw the Future of War. Now It's up to Us to Prepare for It", *The Free Press*, May 8, 2025, available at: www.thefp.com.
15. Quoted in M. Dowd, "Alex Karps Has Money and Power. So What Does He Want?", *The New York Times*, August 17, 2024, available at: www.nytimes.com.



This transformation, therefore, does not entail a replacement but rather the sustainable coexistence of two industrial models. Established players retain a structural advantage in system architecture, certification, industrial sovereignty, in-service support, and risk management. New entrants, on the other hand, call for a faster, more competitive innovation model focused on accelerating the pace of technology and reducing the time between design, testing, and deployment.

Elon Musk takes this logic all the way to the architectural level, through an ecosystem where the network becomes the strategic center of gravity. Starlink thus provides the orbital connectivity backbone used in Ukraine, while Tesla and, in the future, Optimus robotics, provide massive edge nodes through autonomy; xAI with Grok targets the cognitive assistance and data flow management layer. The whole system also relies on a distributed energy infrastructure (Tesla Energy, Powerwall/Megapack) that enhances resilience, as electricity, like data, has now become a lever of coercion. In a world where infrastructure is weaponized, power indeed lies less in an isolated platform than in the ability to orchestrate connectivity, embedded computing, AI, and energy.

It must be acknowledged that Europe, for its part, has missed several opportunities to bridge the gap between technological innovation and military power. Unlike the U.S., which successfully consolidated its industry around the famous “Last Supper” of 1993[16]—the catalyst for a wave of mergers, acquisitions, and vertical integrations that transformed the U.S. defense-industrial complex into a more concentrated ecosystem capable of

16. N. Hooper, “Another Last Supper and a New Era of Defense Giants”, War on the Rocks, May 5, 2025, available at: https://warontherocks.com.

absorbing innovations on a large scale—Europe failed to sustain the momentum initiated with Airbus, Leonardo, and BAE Systems. The 2012 attempt at an EADS–BAE merger,[17] which could have created a transnational champion, failed due to a lack of agreement among European states on governance, public ownership, and sovereignty and security imperatives, relegating European integration to program cooperation and *joint ventures* rather than a capital-based consolidation of the Prime contractors.

On the operational front, it has often been unable to rapidly develop military applications based on civilian advancements: transfer mechanisms, financing instruments, and dual-use supply chains have not been sufficient to capture and militarize the technological breakthroughs originating in the private sector. Nor has Europe succeeded in fostering and sustaining digital giants comparable to their American or Chinese counterparts. Efforts to industrialize software, cloud computing, and data platforms have been more timid, with direct consequences for strategic autonomy and the ability to deploy sovereign defense solutions.

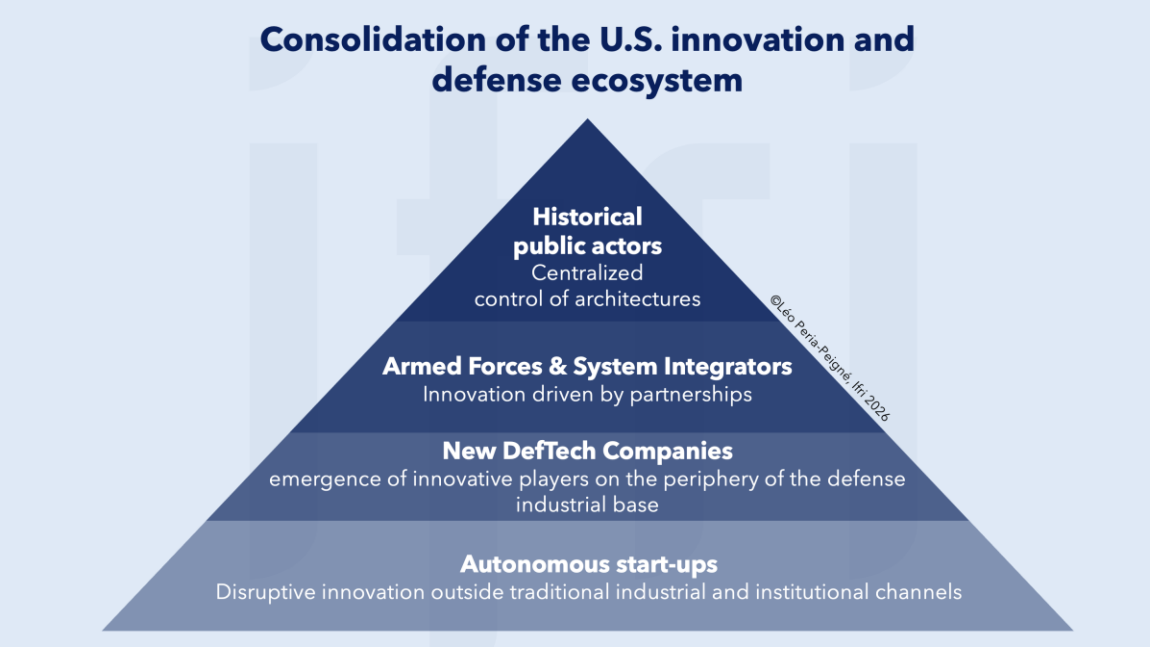
Europe has missed several opportunities to bridge the gap between technological innovation and military power

Across the Atlantic, by contrast, the second decisive phase was precisely the mastery of cloud infrastructure, a strategic linchpin for the storage and processing of sensitive data. At the same time, data and connectivity have become factors of power in their own right, due to the proliferation of sensors (ground-based, airborne, and space-based), the dramatic drop in cost per kilogram to access Earth orbit thanks to reusable launch vehicles, and the emergence of partially privatized intelligence—with commercial firms beginning to provide collection, analysis, or imaging services for the defense sector.

The logical next step was the shift toward *edge computing*, which allows data to be processed and utilized as close as possible to its source—directly on platforms and sensors—to reduce latency, conserve bandwidth, and maintain operations even when connections are degraded. This is the objective of the U.S. Department of Defense's once-controversial Project Maven, which aims to industrialize the use of AI to analyze intelligence streams (particularly imagery and video produced by drones), automate tasks that previously required significant analyst resources (detection, classification, sorting, alerts), and shorten the "sensor-decision-effect" loop.[18] Meanwhile, in Europe, the absence of Big Tech and the fragmentation of architectures have left this strategic

17. "Fusion ratée : BAE Systems n'est 'plus une option' pour EADS" [Merger falls through: BAE Systems is 'no longer an option' for EADS], *Le Monde*, December 10, 2012, available at: www.lemonde.fr.
18. This scaling approach is gradually shifting inference and certain analytical functions toward embedded AI—and thus toward edge—to make the system faster, more robust, and more operational. This is what has enabled players like Palantir to capture the value in the overlay layer, once technical integration and the foundations of data sharing, quality, and security have become sufficiently established within agencies and the military.

segment—platforms, infrastructure, and *de facto* standards—entirely dependent on non-European players.



The final hurdle was cleared with the massive influx of venture capital and the emergence of product-platform integration models into a historically protected market.[19] The Founders Fund, for which Peter Thiel was a key financier and which was the first institutional investor in SpaceX and Palantir, broke down several legal barriers, paving the way for direct investment in weapons technology.[20] In the mid-2010s, as it closed its sixth fund at $1.3 billion,[21] the Founders Fund distinguished itself with contrarian investment theses, including that of DefTech. This shift is embodied in particular by Trae Stephens—a partner at the fund and former Palantir employee—and by Founders Fund's massive support for Anduril, of which he is a co-founder.

Under the banner of "American Dynamism,"[22] conceptualized in early 2022 by Katherine Boyle, founding partner of the venture capital fund a16z, these new-generation investors aim to combine patriotism with investments in DefTech. Josh Wolfe (Lux Capital) is among the investors who, as early as 2019, publicly embraced defense-

19. M. Sion, J. Wenzel, and E. Quirk, "Defense Investment at a Turning Point", Bain & Company, September 2025, available at: www.bain.com.
20. A. Levy, "Peter Thiel's Founders Fund Closes $4.6 Billion Growth Fund", The Consumer News and Business Channel, April 11, 2025, available at: www.cnbc.com.
21. S. Martin, "Peter Thiel's Founders Fund Bags $1.3 Billion", *The Wall Street Journal*, March 25, 2016, available at: www.wsj.com.
22. The idea is to pool investments in companies whose activities serve the strategic interests of the United States—particularly in aerospace, defense, public safety, education, construction, the supply chain, industry, and manufacturing. Since the first American Dynamism Summit in early 2023, investors and companies have been gathering in Washington to strengthen their ties with policymakers. This movement accompanies the growing rapprochement between Silicon Valley and the federal government, marking a new phase of American political capitalism.

focused bets, notably backing Anduril from the outset.[23] Joe Lonsdale's fund (co-founder of Palantir), meanwhile, promotes a company-building model through its 8VC Build program: beyond investment, the fund incubates companies (including in defense, as in the case of Epirus, founded in 2018) before scaling them up.[24] A final example is Thomas Tull's US Innovative Technology, launched in late 2022, which focuses on dual-use players in the sector of "critical technologies of national interest." This is the DNA of SpaceX, Anduril, and other players like Palantir: the ability to merge hardware, software, and defense manufacturing logic at a very large scale.

In Europe, this type of player emerged only later, and in successive waves. EarthCube, now Preligens, paved the way for AI-accelerated intelligence before being acquired by a major industrial group in 2024—a sign of maturity but also of the challenges in breaking free from established industry giants. Complementing this in the "sensors" segment, Unseenlabs integrated commercial space technology into the surveillance chain through detection for maritime intelligence. Then, with Helsing, Stark, and Quantum Systems, a new generation emerged in Germany starting in 2020, connecting software, autonomy, and industrialization all the way to reconnaissance-strike architectures (from intelligence drones to remotely operated munitions), through partnerships with the Primes. More recently, in France, companies like Alta Ares and Harmattan AI are pursuing a more systemic ambition. They aim to transform Command and Control (C2), industrialize autonomy, and build capabilities in the attrition and low-end-of-the-spectrum weapons segment on a European scale. The key challenge, then, is to give them the strategic and industrial space to grow without being absorbed.

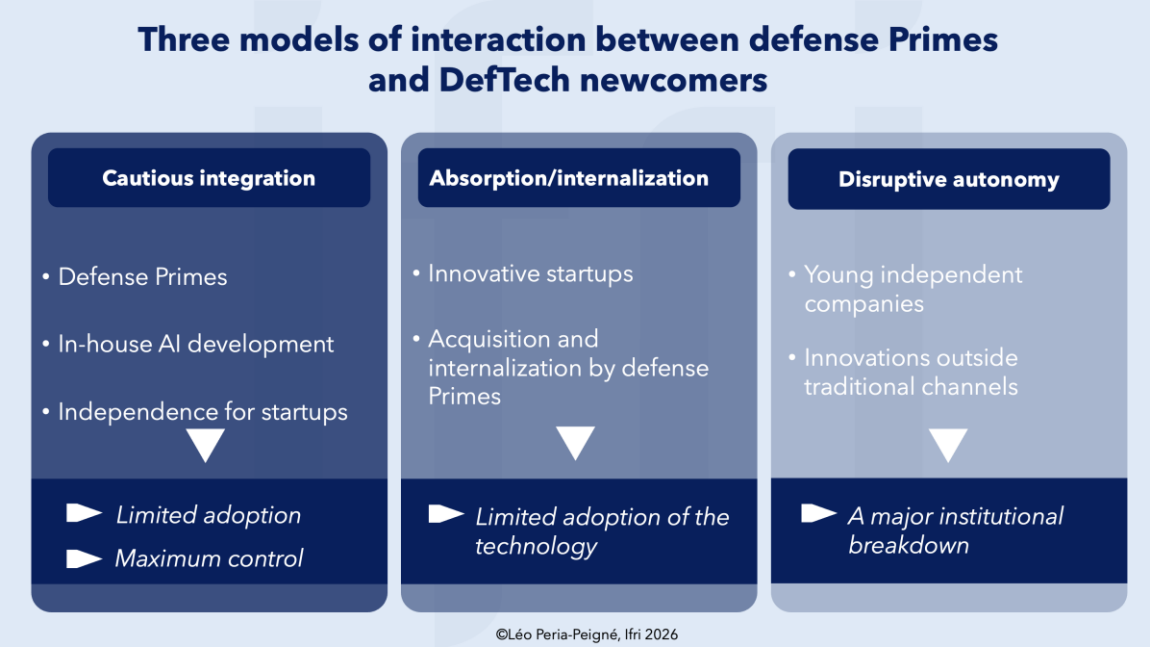
This is the DNA of SpaceX, Anduril, and other players like Palantir: the ability to merge hardware, software, and defense manufacturing logic at a very large scale

A clash between the old and the new?

Traditional manufacturers rely on a sequential model, backed by firm contracts, standardized milestones, and long cycles. New entrants, on the other hand, seek to bypass intermediaries and interact directly with users, using iterative approaches. They invest without guarantees, iterate quickly, and rely on software updates and incremental value creation.

23. J. Wolfe, "A Serious Investment in a Serious Company: Anduril", Lux Capital, October 4, 2019, available at: www.luxcapital.com.
24. J. Lonsdale, "Our Duties as Defense Technologists", Joe Lonsdale Blog, November 2, 2023, available at: https://blog.joelonsdale.com.

As a result, the defense AI ecosystem has thus far been characterized by structural fragmentation, stemming from the clash between legacy defense industrial base players and these emerging players. The former, concerned with preserving their financial value, are reluctant to collaborate with startups, fearing that the latter will capture a disproportionate share of the value. At the same time, they limit their own risk-taking, investing only when public contracts secure the exploration of new technologies.



As a result, three models of interaction between them have emerged. On the one hand, major defense industrial base players are seeking to gradually incorporate AI capabilities, without relying on startups, and in a cautious and limited manner.[25] On the other hand, certain new entrants, bringing significant technological innovations, have been acquired or internalized by these same large groups, allowing for partial dissemination of the technology while concentrating control.[26] Finally, a third category of startups is developing autonomously, outside traditional industrial and institutional channels, exploring disruptive solutions without being integrated into the conventional framework.

Interactions between "legacy" and "modern" systems are thus hampered by a lack of mutual trust and by obstacles that are institutional (security, clearances, compliance), contractual (intellectual property, liability, procurement cycles), organizational (integration into existing architectures), and, in some cases, reputational (political, media, or internal acceptability).

25. MBDA has thus created the "Neode Systems" structure to accelerate the development and integration of AI into the group's systems. This is also the approach taken by Thales with cortAIx, or dedicated R&D initiatives at BAE Systems and Leonardo.
26. For example, Safran acquiring Preligens (now Safran.AI) or BAE Systems integrating BISim (simulation/training).

Across the Atlantic, however, the opposition between "old" and "new" has become partly artificial. Major contractors have healthy order books, while new entrants are financing themselves through IPO trajectories made credible by already significant public contracts and by capital's appetite for defense technology. Under these conditions, the narrative of "creative destruction"—in which the new automatically replace the old—does not hold up to scrutiny. Competition is heavily regulated by the state, industrial collaborations are frequent, and the boundaries between public and private sectors are deliberately blurred.

The real point of tension, then, lies in Europe. Lacking a unified market and comparable financing and industrialization capabilities, Europeans have neither the critical mass nor the scaling mechanisms to simultaneously support established manufacturers and sovereign new entrants. Many European startups continue to struggle. Despite technological successes, they fail to overcome the industrial, contractual, and financial barriers to scaling up, which hinder their sustainable integration into the defense industrial base and consequently limit the coherent integration of AI into the European defense value chain.

In France, the response to this restructuring of the defense industry is organized around three pillars:

- a sovereignty pillar, focused on the most critical and sensitive programs;
- a cross-dependence pillar, aimed at controlled and reversible cooperation;
- a market pillar, based on the agility of startups, venture capital, platform-based approaches, and open standards.

The government is also shifting its approach to the issue of "weaponization" with the creation of the Ministerial Agency for Defense Artificial Intelligence (AMIAD). Nevertheless, in the absence of an explicit governance regime, an integration doctrine, and structured public funding, these initiatives risk failure, fragmentation, or dilution. The challenge, therefore, is not to choose a single model, but to coordinate multiple innovation frameworks into a coherent trajectory.

Toward a European strategic hybridization

The "traditional" and "modern" models are not, in fact, incompatible: they serve different functions, just as special forces complement conventional forces. The question that arises, however, is where the primary military advantage lies—in intangible capabilities or in equipment. If it lies in the intangible, the historical players will logically, over time, become interchangeable suppliers, and the issues of sovereignty and R&D will be relativized. This tension thus calls for a conscious synthesis, by enabling open platforms and envisioning a governance model capable of orchestrating multiple timeframes.

The ongoing capabilities revolution represents a historic opportunity for hybridization. Provided we do not mimic the Californian model, it is possible to build a pragmatic alliance between established players and new entrants, where each finds its place in a reimagined value chain. To the former, industrial security, integration and industrialization, scaling up, and controlled quality chains; to the latter, agility, innovation, and speed of adaptation.

It is possible to build a pragmatic alliance between established players and new entrants

The return of high-intensity warfare imposes a dual constraint on Europe. On the one hand, it is necessary to significantly increase production capacities to rearm Europe and rebuild its strategic depth. On the other hand, it is essential to integrate technological innovation more rapidly into weapons systems and combat doctrines. While the U.S. has had nearly two decades to transform its defense industrial base, Europe must accomplish these steps in a significantly shorter timeframe, even as Washington now positions itself as the "arms shop" and provider of the information architecture for its allies, offering them hardware, software, and doctrine alike.

Faced with this dual challenge, Europe has no choice but to combine two complementary approaches: "decision-making tools" (high-end) and "tools of attrition" (smart and affordable mass). The challenge is not to choose between the two, but to combine them: the low-end provides mass, saturates the battlefield, secures positions, and can be rapidly replenished, while the high-end delivers the decisive effect at the critical moment. This complementarity is also industrial: the high-end establishes credibility, while the low-end ensures volume. We must simultaneously maintain a portfolio of major platforms whose performance is recognized but whose design remains relatively non-modular and poorly adaptable, while embracing the ongoing revolution.

This doctrinal and industrial restructuring is based on a new capacity framework, which involves mass production, modularity, the "target cost"[27] approach as a design parameter, technological sovereignty, functional safety, robustness, and the increased integration of AI as an operational multiplier. Seven key initiatives must be prioritized to achieve this:

- Diversify the ecosystem and formalize hybridization, avoiding the reduction of new entrants to just a few "champions." It is essential to foster a heterogeneous ecosystem comprising startups, SMEs, and mid-sized companies—including dual-use entities—and to clarify the value chain with established manufacturers by defining "who does what" (critical components, system integration, testing, and qualification). To achieve this, standard clauses can be established regarding IP, liability, cybersecurity, market access, exports, and revenue sharing to reduce mistrust and accelerate integration.
- Standardize open "plug-and-fight" architectures. This involves implementing reference architectures (standards, APIs, data models, cybersecurity, access identities, traceability requirements) to "plug in" multiple solutions without proprietary lock-in. A common certification for levels, profiles, and compliance testing is also desirable, as well as a clear governance regime that sets the reference level and mediates changes.
- Accepting upfront investments without prior contractual requirements, by funding demonstrators and industrial capabilities before the order is placed (prototyping, testing, pre-production), in order to reduce the time between the idea and the capability, and to ensure a smooth ramp-up.
- Make data a shared sovereign capability by establishing a security "data commons" framework (catalog, classification levels, usage rights, anonymization, traceability) to train and evaluate models, test interoperability, and accelerate feedback loops.
- Focus efforts on a small number of "critical technologies" and adopt an evidence-based approach, retaining only a few foundational priorities (applied AI, autonomy, robotics, communications, electronic warfare, etc.) and enforcing a discipline of progress: short roadmaps, quarterly reviews, rapid decisions to halt or pivot, and evolving reference frameworks should be prioritized.
- Strengthen scaling up by mobilizing European corporate venture capital aligned with sovereignty imperatives and capable of financing not only R&D but also industrialization (supply chain, certification, production, export); and by planning for compatible exit strategies.

27. The target cost is no longer a constraint addressed at the end, but a design parameter from the outset: the manufacturer defines the acceptable unit price (and the full lifecycle cost), then designs the system—architecture, materials, sensors, performance level, industrialization, maintenance—to meet this cost while remaining militarily relevant.

- Reduce bureaucratic friction through lean teams with a clear mandate (decide quickly, buy better, integrate faster), with accelerated testing and qualification processes, and explicit accountability for delivering capabilities.

Conclusion

For France as well as for Europe, the defense economy now rests on the coexistence of two distinct markets. On one hand, there remain strategic weapons systems with long lifespans—air, naval, or land-based platforms—that are highly technological, costly, and designed to last for several decades. On the other hand, a new market is emerging, characterized by expendable capabilities, mass-produced, with low unit costs and rapid innovation cycles, of which drones in Ukraine are the most visible example. As the warfare of tomorrow moves toward saturation, the economy of scale, and industrial responsiveness, the balance of power risks being profoundly redistributed, and traditional players see their leadership challenged. This lack of clear articulation between the "old" and the "new" now constitutes a real obstacle: it fragments efforts, slows innovation, and weakens Europe's ability to remain competitive against powers that have already bridged this gap.

In this context, AI cannot be viewed as a turnkey solution: it is only operational when integrated into existing chains, sometimes through modest increments, sometimes at the cost of a complete overhaul of software and decision-making architectures. This is precisely why the search for appropriate European approaches—industrial, doctrinal, and technological—constitutes a major strategic challenge. Without the ability to combine technological capital with mass production, Europe could find itself marginalized in future high-intensity conflicts. This requires an active role for public authorities, not to arbitrate between "old" and "new," but to organize their hybridization.

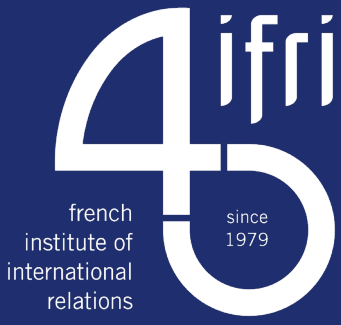
Alexandre Papaemmanuel *is an adjunct professor at Sciences Po Paris and a defense science advisor for the Security & Defense specialization at the School of Public Affairs. His work focuses on intelligence, defense, and new technologies at the intersection of strategic analysis, operational challenges, and public policy. He is vice president of French Intelligence & Cyber Studies and a board member of Defense Angels.*

Laure de Roucy-Rochegonde *is the Director of Ifri's Center for Geopolitics of Technology since February 2024. Her work focuses on the military applications of artificial intelligence, normative conflict, and arms control. In October 2024, her first book, titled* La Guerre à l'ère de l'Intelligence artificielle : quand les machines prennent les armes (PUF)*, was published.*

How to cite this publication:

Alexandre Papaemmanuel and Laure de Roucy-Rochegonde, "Europe at the Crossroads of DefTech: Rethinking the European Defense Innovation Ecosystem", *Ifri Memos*, Ifri, February 16, 2026.

ISBN: 979-10-373-1225-9



27 rue de la Procession
75740 Paris cedex 15 – France

Ifri.org