DGTL
Makers
&Shapers

DIGITAL AND DEFENCE INNOVATION FOR EUROPE'S STRATEGIC AUTONOMY

CONTENT

INTRODUCTION

Following the political guidelines for the new Commission presented by President Ursula von der Leyen on July 18, 2024[1], the EU defence policy entered a new phase of acceleration. The political guidelines identified defence as a priority and a key sector for completing the single market. Achieving strategic autonomy will require significant efforts, including the establishment of a "European Defence Union". The context, within which the EU policy-defence making process is accelerating, is characterised by the geopolitical shifts occurred during the last decade, amplified by the Russian war of invasion against Ukraine, and culminated most recently with the change of the US foreign policy orientation introduced by the new Trump administration. This context and the most recent developments have led the EU to launch the Re-Arm EU plan, unveiled on March 4, 2025, by President Ursula von der Leyen[2], and further fleshed out on March 19, 2025, in the White Paper on the Future of European Defence[3].

As defence becomes a more explicit EU policy and investment priority, a central challenge lies in the integration and governance of dual-use technologies. These are officially defined in Article 2 (1), of Regulation (EU) 2021/821[4] as follows: " 'dual-use items' means items, including software and technology, which can be used for both civil and military purposes, and includes items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery ...". So, dual-use should be defined as technologies with equal potential for both civilian and military markets. In this report when using this expression we refer to technologies such as Artificial Intelligence (AI), autonomous systems, sensing, quantum computing, robotics, Internet of Things, advanced addictive manufacturing, secure 5G and 6G telecommunication networks, as well as access to, and use of semiconductors. Although more applied to the military there are also post-quantum encryption, Unmanned Aerial Vehicles (UAVs), and electronic warfare.

Dual-use capabilities are increasingly viewed not just as by-products of innovation, but as strategic assets essential for both economic resilience and military readiness. Also the Commission 2025 Foresight Report underscores the importance for EU security of civil-military synergies and places amongst the 8 actions toward resilience 2.0 that of developing a technology-savvy forward-looking approach to internal and external security capitalising on such civil-military synergies[5]. As such, ensuring their development, financing, secure, and ethical use is emerging as a core dimension of EU defence and industrial policy. Very recently (16 July 2025) in the Commission proposal for the establishment of a European Competitiveness Fund it is stated that 'It is therefore imperative to seek measures to better exploit the potential civil-defence synergies and of dual-use technologies'[6]. From AI and semiconductors to space infrastructure, cybersecurity, and secure advanced telecommunication networks, many technologies developed in the civilian sector are now strategic assets in defence contexts. The EU's challenge is to harness and govern these dual-use technologies effectively and ethically: ensuring they strengthen military readiness while also supporting competitiveness, innovation, and resilience in civilian markets, as well as in such a way that ethical standards define what these technologies can and cannot do, especially for AI and autonomous systems. This imperative is shaping emerging policy instruments, investment priorities, and regulatory frameworks.

Already in November 2023, President von der Leyen emphasised the need to maximise the EU's dual-use potential: "While we strengthen our defence-specific R&D, we should also better integrate civilian technologies into our defence industrial base. There is so much vital innovation with defence applications that emerges from civilian activities. It is now important that we connect the dots."[7] Compared to the past, technologies supporting

security and defence capabilities are increasingly derived from the civilian sector, where private investment is higher, indirect costs are lower, and R&D cycles are faster. As noted by a recent NATO Report: "Countries that successfully integrate and commercialise such technologies gain significant economic and strategic advantages. To maintain a technological edge, NATO allies must reinforce innovation funds, while strengthening partnerships with the private sector and universities to harness emerging technologies, particularly artificial intelligence, for both security and economic resilience."[8]

Proof of the strengthened innovation-defence nexus is that "international and intergovernmental organisations like NATO or the EU and nations such as the US have rushed to establish novel arrangements for innovation-driven security governance: innovation hubs, accelerators, innovation units, and innovation agencies"[9]. In 2015 the US Department of Defense (DoD) established the Defense Innovation Unit (DIU) for assisting companies with transitioning commercial solutions to Defence Department users in six technology domains, including artificial intelligence/machine learning, autonomous systems, cyber, energy, human systems and space. In 2022, the US DoD established the Chief Digital and Artificial Intelligence Office (CDAO) to scale up Pentagon's innovative power via the closer integration of advances in AI systems, data analytics and other digital technologies across the DoD[10]. Also in 2022 NATO launched DIANA (Defence Innovation Accelerator for the North Atlantic) to ensure that NATO harnesses the best of dual-use innovation for transatlantic defence and security. DIANA aims to create a transatlantic innovation platform, establishing the first multi-sovereign venture capital fund, the NATO Innovation Fund (NIF), to provide strategic investments in start-ups developing dual-use deep-tech[11]. Still in 2022 (May 17) the Hub for EU Defence Innovation was established within the European Defence Agency (EDA) as a platform to stimulate, facilitate and support cooperation on defence innovation among Member States while ensuring synergies with related European Commission activities. In that occasion, EDA Chief Executive, Jiří Šedivý said: "With the rapid development of new and often disruptive technologies and their fast weaponisation, innovation has become a geostrategic factor shaping the international security environment and the global balance of power"[12].

The new geopolitical context is one where the system of international relations is undergoing changes of a significance not seen after the end of the World War II in 1945, with the orders emerged in 1945 and after the end of the Cold War allegedly crumbling. The security of the EU and its citizens is first threatened by large-scale war at its borders and hybrid attacks within its borders. In other words, Russia represents a main threat, being the most heavily armed state in Europe and currently running a war economy. According to the cited White Paper[13], Russia in 2024 spent in defence 40% of its federal budget or close to 9% of GDP. On the other hand, while at the recent NATO summit in The Hague (25 June 2025) allies agreed to invest in the future 5% of GDP in defence, as of 2024 11 EU countries out of 27 had not yet reached the previous NATO 2% target[14]. The cited White Paper underscores that part of the new geopolitical context is a new global technology race, as "technology diffusion for commercial purposes must be reconciled with more rigid technology ecosystems to advance national security objectives. The EU's strategic competitors are heavily investing in this area"[15].

The Re-Arm EU plan aims to mobilise around €800 billion over the next four to five years to reach European defence readiness by 2030. While most of the funding would come from Member States increasing their national spending on defence and security, €150 billion would come from a new defence instrument (Security and Action for Europe, SAFE), allowing the Commission to borrow from capital markets to issue bonds and lend to Member States. The Commission has also proposed three additional measures: mobilising more private capital, adapting the European Investment Bank's (EIB) mandate, and incentivising defence-related investments in the EU budget. A key pillar of the plan, still

not adopted, is the proposal to broaden the EIB mandate as to include financing for dual-use companies - i.e. those with less than 50% of their revenues coming from defence-related activities. As stated by Guntram Wolff, senior fellow at the economic think-tank Bruegel, "In a time of rising defence expenditures, that's quite a constraint because many dual use companies cannot be funded by the EIB (...), so I think that there is scope to change the mandate of the EIB and use the EIB as a vehicle to fund companies that have a severe gap in their funding from private banks and capital markets"[16].

The cited White Paper underscores that part of the new geopolitical context is a new global technology race in applications that are: "key inputs for both long term economic growth, and military pre-eminence. Boosting innovation is key for this. As such, technology diffusion for commercial purposes must be reconciled with more rigid technology ecosystems to advance national security objectives. The EU's strategic competitors are heavily investing in this area"[17]. To this purpose investments in research, development, and technology must be stepped up especially with efforts and resources channelled through common European projects[18].

This report aims to provide insights and suggestions on how the promises of dual-use technologies can be realised and the challenges overcome by developing future scenarios. It focuses in particular on key digital technologies with significant dual-use potential. It does so, however, considering also broader trend of defence expenditure. It builds on secondary sources, analytical and theoretical reasoning, and experts' knowledge. Inputs on a draft of this report was obtained by 42 experts during two roundtables held, respectively, July 14 and 23 2025. In Section 2 the report provides a contextualised analysis of the economic and security dynamics of dual-use technologies. Section 3 elaborates four future scenarios to illustrate how dual-use could evolve under different geopolitical, technological, and regulatory conditions. The scenarios are then assessed in Section 4, which concludes with policy-relevant implications and recommendations.

DEFENCE AND DUAL-USE TECHNOLOGIES IN GEOPOLITICAL CONTEXT

DEFENCE EXPENDITURES AND TECHNOLOGY INVESTMENTS: TRENDS AND STATE OF PLAY

In order to understand the current dynamics of defence policy in general and of the role of dual-use technology, it is useful to look historically at the broad trends in defence expenditure that reflect shifting geopolitical contexts. To look at historical trends we use the Military Expenditure Database held by the Stockholm International Peace Research Institute (SIPRI), which contains consistent time series on the military spending of countries worldwide for the period 1949–2023[19]. For the sake of brevity and ease of exposition we look at the trends in defence expenditure as a share of GDP for the US and for the four largest European countries (France, Germany, Italy, and UK).

As illustrated in the figure above, defence expenditure began to decline across all countries following the end of the Cold War. In particular, European countries significantly reduced their military budgets, redirecting what became known as the "peace

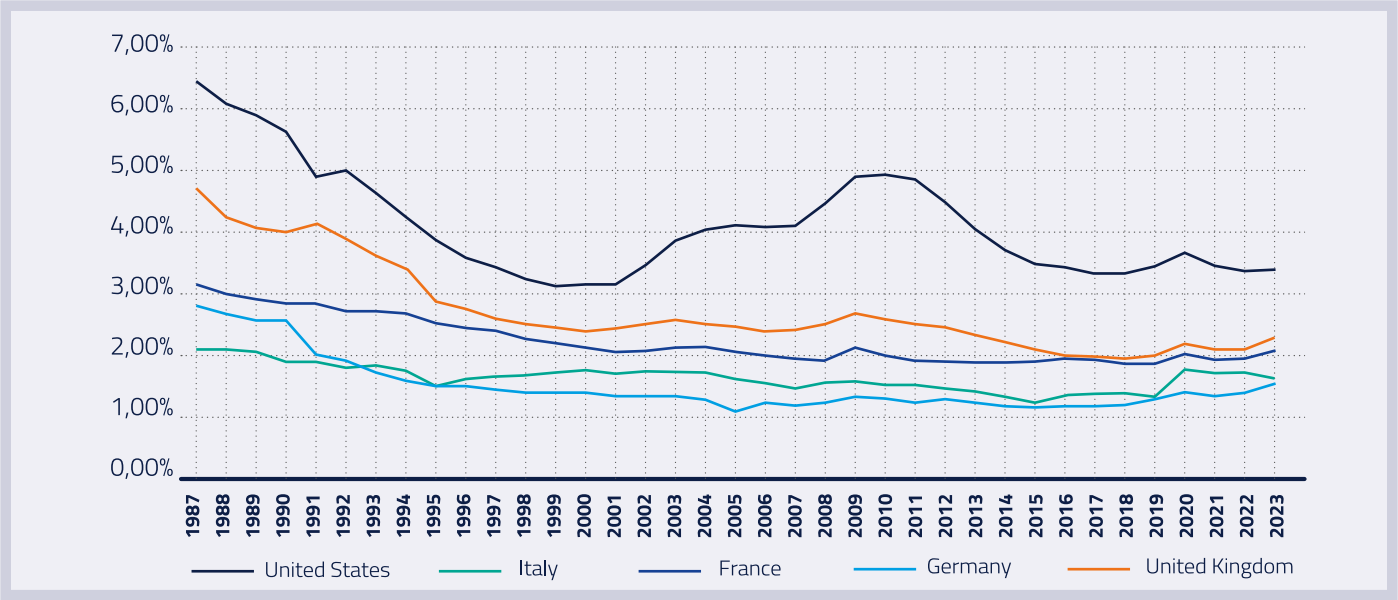

Figure 1 Defence expenditure as a share of GDP in selected countries: 1987-2023, Source: SIPRI

dividend" toward other pressing policy priorities. This downward trend was further reinforced by the economic and financial crisis of 2007–2008, which placed additional constraints on public spending. However, since 2022 defence budgets, especially in the four European countries highlighted, have begun to rise sharply in response to the Russian invasion of Ukraine and the shifting geopolitical landscape. If we compare current expenditure levels with those of the 1950s, when the Cold War was in full swing, the differences are sharp. For instance, the US spent 10% of GDP in defence in 1958, while only 3.3% in 2023, the United Kingdom spent 7.62% in 1958 as compared to 2,26% in 2023, France spent 5.69% in 1958 as compared to 2% in 2023, and similar differences can be observed for Germany and Italy. Therefore, the recent increase in military expenditure both in the US and Europe came after a fairly long period of decrease, especially in Europe. In Europe, in fact, while defence expenditure and related components have increased markedly between 2022 and 2024, this is not yet sufficient to fill the gaps cumulated in decades of spending cuts and underinvestment in defence[20]. In the 2024 Draghi Report the defence spending/investment gaps was estimated at EUR 500 billion[21]. The report outlined several structural weaknesses in the EU's Defence Technological and Industrial Base (EDTIB) affecting its competitiveness such as fragmentation, insufficient public defence investment and limited access to financing. Likewise the Draghi Report, also the Niinistö Report[22] stressed fragmentation and lack of European level collaboration as key sources of inefficiencies hindering the capabilities of the EDTIB and imposing additional (duplicating) costs on all Member States. It has been calculated that in the 2006-2022 period the cumulative spending gap (comparing actual spending against the NATO 2% target) has been of about EUR 1 250 billion in nominal prices, corresponding to more than EUR 1770 billion in constant 2024 prices[23].

Below we use data from the European Defence Agency (EDA) reports (an in particular the latest one[24]) to characterise the state of play of EU defence expenditure and of the European Defence Technological and Industrial Base (EDTIB).

EU27	2021	2023
Total Defence Expenditure	€ 217.150 Mln	€ 278.573 Mln
Total Defence Expenditure as % of GDP	1,5%	1,6%
Defence Investment	€ 53.013 Mln	€ 71.975 Mln
Defence Equipment Procurement Expenditure	€ 43.818 Mln	€ 61.314 Mln
Defence R&D Expenditure	€ 9.195 Mln	€ 10.661 Mln
Defence R&T Expenditure	€ 3.561 Mln	€ 4.038 Mln
Collaborative Defence Equipment Procurement Expenditure	€ 9.875 Mln	-
European Collaborative Defence Equipment Procurement Expenditure	€ 7.895 Mln	-
Collaborative Defence R&T Expenditure	€ 262 Mln	€ 265 Mln
European Collaborative Defence R&T Expenditure	€ 248 Mln	€ 242 Mln

Table 1 EU27 Defence Expenditure [25] , Source: https://eda.europa.eu/docs/default-source/documents/defence-data/defence-data-2023.xlsx.

So, in 2023 defence expenditure reached about EUR 279 billion representing a sizeable increase compared to 2021 (a 28% increase) as a result of the efforts that Member States have done to bolster their armed forces' fighting capabilities in response to Russia's war of aggression against Ukraine. Despite such efforts, defence expenditure accounted for 1.6% of GDP, still falling short of the previous NATO 2% target. For 2024 the Coordinated Annual Review on Defence (CARD)[26] estimates that total defence expenditure at €326 billion in 2024, which corresponds to 1.9% GDP, thus, closer to NATO's previous 2% target.

Defence investments (equipment procurement, defence research and development and its component defence research and technology) reached in 2023 EUR 72 billion, which is 26%

of total defence expenditure and is well above the 20% target. In 2024 defence investments are expected to grow and reach EUR 30 billion (or 30% of defence expenditure). It must be noted that the current surge in investments, caused mostly by the Russian invasion of Ukraine, came after a prolonged period of underinvestment as Member States invested steadily less than 20% after the 2008 financial crisis for ten consecutive years. Equipment procurement (about EUR 61 billion in 2023) accounts for 80% of defence investments, and very often was spent in Commercial Off-The-Shelf (COTS) products procured from non-European manufacturers given existing capability gaps, thus, weakening the European Defence Technological and Industrial Base (EDTIB)[27]. In this respect, it has been estimated in an IRIS policy paper dated 2023 that from a total of EUR 75 billion spent by Member States for equipment between June 2022 and June 2023, 78% has been procured from outside the EU, out of which almost 63% from the US[28] . As noted: "The growing trend of non-European COTS procurement risks weakening the EDTIB further with the associated challenges to the EU's strategic autonomy, interoperability of defence equipment, and long-term consequences for European cooperation in related capability areas"[29]. The trend for quick procurement of COTS from outside of the EU is clearly slowing down European collaborative equipment procurement, which is probably perceived as more complex and time-consuming in the face of short-term necessity. Member States had agreed the target of having European collaborative defence equipment procurement account for at least 35% of total equipment spending. While data on this item are not available for 2022 and 2023, in 2021 European collaborative defence equipment procurement (EUR about 7.8 billion) amounted to 18% of the total, quite far from the 35% target. Defence research and development in 2023 reached almost EUR 11 billion representing a big increase compared to the low peak of 2016 (more than doubled) but is still insufficient to compensate prior underinvestment and to keep up with the pace of other players such as the US and China. In 2023, the United States of America allocated around €129 billion to Research, Development, Test, and Evaluation (RDT&E)[30]. This category saw the most significant increase in U.S. military spending in 2023, emphasizing the importance that the United States placed on defence RDT&E[31]. According to available data, China's defence R&D spending could amount to €21 billion in 2023[32]. The investment in defence R&D by the US and China testify to the importance of supporting new and sophisticated technologies. Moving to defence research and technology (R&T) it is worth recalling that this category includes expenditure for basic research, applied research and technology demonstration for defence purposes. In 2023 it amounted to EUR 4 billion, which is 1.4% of total defence spending and below the agreed target that of 2% of total defence spending. European collaborative R&T with €242 million in 2023 accounted for 6% of

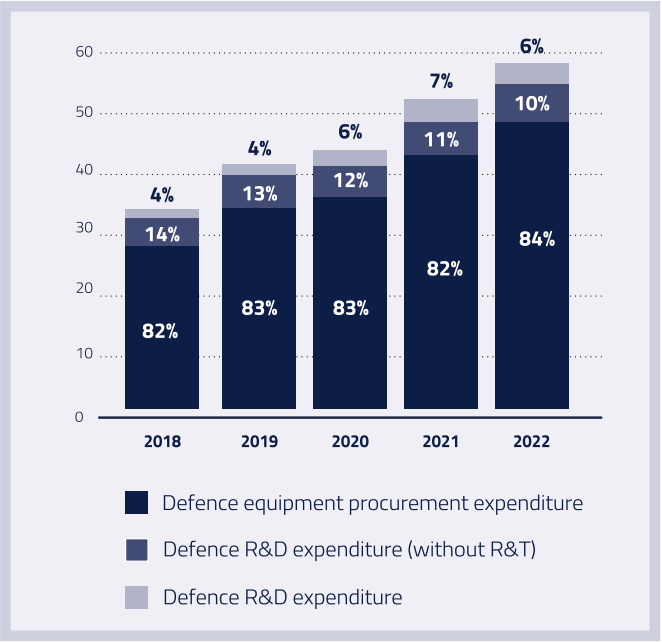

Figure 2 EU Defence investment decomposition, by investment type, Source: DG Research and Innovation, based on EDA Defence Data 2022

total defence R&T expenditure, falling short of the 20% collective benchmark agreed by Member States. Overall, recent increases are significant but insufficient to recover from past underinvestment or match the scale and strategic focus of other major powers[33]. Moreover, as shown in the Figure below, spending on basic and applied research, and technology validation has fallen behind.

While total defence spending across EU Member States has increased steadily over the past decade, fragmentation remains a key challenge. It has been noted that potentially the EU defence market could be the third largest domestic market and in line of principle should enable EU industrial players to rip economies of scales and the efficiency gains deriving from a large market and supporting competitiveness, innovation, and production capacity[34]. Yet, it has been observed that this market "remains largely fragmented along national borders with limited coordination and cooperation and the associated substantial wasteful duplications"[35]. Defence companies are mostly structured to suit national priorities with demand mainly expressed by national governments from their national industries, which profit from close relationships with their respective governments[36]. This has led to a high number of national defence companies, operating in small markets, with insufficient production levels to cope in the current geopolitical environment. This fragmentation leads to costly duplication, renders logistics and transnational cooperation on maintenance more difficult and hampers interoperability. One clear and concrete indication of fragmentation is provided by the data on collaborative European procurement of defence equipment seen earlier. Member States in 2007 at the EDA Ministerial Steering Board the EU Member States agreed that they should aim at European defence cooperative procurement reaching 35% of their total defence equipment procurement. But EDA data show that this benchmark has never been even remotely approached, with the percentage of collaborative procurement remaining around maximum 20%[37]. This trend shows that EU Member States' demand for defence equipment, despite its recent increase, remains fundamentally fragmented and thereby deprives the EDTIB from the benefits of a truly functional EU defence market. The 2022 CARD report notes that 'cooperation remains the exception rather than the norm', highlighting that a collaborative approach is mainly used when it coincides with national plans, would benefit national defence industries, or consolidates a strategic partnership[38]. The current increase in defence expenditure for equipment procurement has gone to COTS product often from outside the EU, thus hindering the development of a truly European procurement collaboration. And the same apply for defence R&D. So, opportunities are missed to leverage European economies of scale to lower unit costs. Low and fragmented Member States' defence spending on innovation negatively impacts emerging disruptive technologies that are vital for future defence capabilities.

France is the only EU country with 2 dedicated public venture capital fund focused explicitly on defence and dual-use startups. Launched in 2018 with €100M, Definvest a specialised equity fund managed by France's public investment bank, Bpifrance, focused on start-ups and SMEs regarded as strategic for French armed forces equipment. Launched in 2021 and with €275M, Fonds Innovation Défense is a specialised equity fund managed Bpifrance, focused on start-ups with dual-use technologies like quantum, AI or space regarded as "of interest" for French armed forces equipment. Moreover, in March 2025, the Economy Minister Eric Lombard announced that Bpifrance will launch in October a new fund of up to €450 million for people to invest their money in defence companies "for the long term". The government aims to raise 5 billion euros in additional public and private funding[39].

There are other relevant initiatives in other EU countries worth mentioning:

- **Germany.** The Cyber Innovation Hub of the Bundeswehr (CIHBw)[40] supports the digital transformation of the Bundeswehr and act as an interface with the startup ecosystem. With the implementation of a total of over 160

innovation projects, the CIHBw sees itself as an innovation driver for the armed forces. It is the first military digital innovation unit in Europe and a role model for comparable units in other German federal ministries and authorities.

- **The Netherlands.** Defence innovation in the Netherlands is being boosted by a new strategy, the Defence Strategy for Industry and Innovation 2025-2029, which focuses on scaling up innovation and production through public-private partnerships and strategic investments. Key initiatives include the Defport[41] platform to accelerate innovation and production, the SecFund[42] to finance dual-use tech startups, and collaborative projects with the private sector to develop new technologies in areas like smart materials, space, quantum technology, intelligent systems, and sensors.
- **Spain.** The COINCIDENTE program is run by the Spanish Ministry of Defence and supports collaboration with startups and SMEs with defence-relevant innovation.
- **Latvia.** Latvia is leading the Drone Coalition initiative to coordinate international efforts in supplying Ukraine with drones and boosting Europe's drone production[43].

Box 1 National initiatives

As noted in one of the earlier cited EDA report[44], steadily increasing defence R&D is strategically crucial for the EU and its Member States to stay at the frontier of new technological advances and keep the pace of geopolitical global players. Such investment is also important for the competitiveness and long-term viability of the European defence industry. To this purpose, collaborative European projects represent the ideal solution, as the pooling of resources would enable large technological advanced R&D projects requiring large investment hardly within the reach of single countries. Against this backdrop, the European Defence Fund (EDF) has emerged as a central instrument to address these challenges and foster a more integrated approach. Introduced in 2021, the EDF is the European Commission's flagship programme for collaborative defence R&D, aiming to boost innovation, promote interoperability, and enhance the competitiveness of Europe's defence technological and industrial base. With a total budget of €7.3 billion for 2021–2027, the Fund supports cross-border cooperation among companies and research institutions. The Fund also allocates between 4% and 8% of its budget to disruptive technologies, ranging from quantum sensing to autonomous systems and advanced materials. The 2025 Work Programme, adopted in March 2025, allocates €1.065 billion to collaborative R&D projects. This significant investment is further reinforced by a €1.5 billion top-up from the Strategic Technologies for Europe Platform (STEP), aiming to boost investment in strategic sectors including digital technologies, deep-tech innovation, clean energy, and biotechnologies. The EDF enables the EU Defence Innovation Scheme (EUDIS)[45], which is an instrument to strengthen SMEs defence innovation in the European Union. The 2025 programme, among other things, include: technological challenge in Artificial Intelligence; R&D calls fostering civil-defence synergies in space, energy resilience, ground combat, and cyber. The EDF does not operate in isolation. It is embedded in a broader EU innovation ecosystem that includes the European Innovation Council (EIC), which supports dual-use technologies and deep-tech, the European Investment Bank (EIB), which provides equity and loans for scale-ups, coordination mechanisms with NATO's €1 billion Innovation Fund, as well as national initiatives such as the Defence Innovation Accelerator for the North Atlantic (DIANA).

DIANA and the NATO Innovation Fund (NIF) are two legally separate entities, with different mandates and activities working toward a common purpose.

- DIANA, or the Defence Innovation Accelerator for the North Atlantic, is a NATO initiative focused on accelerating dual-use innovation across the Alliance. Its primary mission is to connect innovators with operational end-users to foster a transatlantic ecosystem supporting groundbreaking, deep-tech solutions to critical defence and security challenges.
- The NIF is a €1 billion venture capital fund, backed by 24 NATO

Allies, that invests in deep tech to address challenges in defence, security, and resilience. The NIF is a privately-owned, for-profit entity which has received approval to use the NATO name. NIF is a standalone venture capital fund, and its capital comes from 24 sovereign countries in the NATO alliance. NATO as an organisation is not invested financially or involved in decision-making.

Box 2 DIANA and the NATO Innovation Fund

While the EDF represents a significant step forward for coordinated EU-level investment in defence and dual-use technologies, it is important to recognise its relative scale. Even with the €7.3 billion allocated for 2021–2027, which corresponds approximately to 1 billion a year, the EDF accounts for only a small share of overall defence-related R&D spending in Europe. Most investment in dual-use technologies still occurs at the national level, through both civilian and military R&D programmes, as well as through private sector initiatives in areas such as artificial intelligence, advanced semiconductors, quantum computing, space, and cybersecurity. Estimates suggest that civilian R&D spending across the EU reached around €381 billion in 2023[46], with only a small fraction of that directed toward security or defence applications. In comparison, public defence R&D in the EU27 amounted to €11 billion in 2023, with significant variations between Member States. Therefore, the EDF's contribution represents roughly 15% of this annual public defence R&D.

When placed in a global context, Europe's progress appears modest. The scale and strategic coordination of defence innovation efforts in other major powers, particularly the U.S. and China, highlight the gaps the EU still faces. The United States spent over $130 billion annually on military R&D in recent years—more than ten times the combined defence R&D budgets of all EU Member States[47]. The U.S. Defense Advanced Research Projects Agency (DARPA) alone has an annual budget of over $4 billion, focused exclusively on high-risk/high reward defence innovation. China does not publish official figures but estimates place its military R&D spending at $20–30 billion annually, with a strong focus on AI, quantum, hypersonic, and cyber[48].

With respect to funding, a recent study (2024) commissioned by Directorate-General for Defence Industry and Space[49] and focussing on defence SMEs access to capital investments (based also on a survey with representative of defence SMEs) provides some interesting insights that are worth summarising here.

First, while dual-use technologies with application in the defence sector have attracted the interest of Venture Capital, nonetheless Defence SMEs still face higher barrier (as compared to SMEs in general) for accessing finance. Second, the size of this financial market remains very limited in the EU, compared to the US and UK. In particular, the EU lacks an ecosystem of specialised funds. Third, potential investors stress as barrier: complexity and length of procurement procedure in the defence sector limiting visibility of market potential; sector-specific regulations introducing complexities and higher costs. This aspect is crucial since, as noted by experts during the two roundtables, it deprives investors and startups of those demand signals that increase predictability. Fourth, barriers derive from a too strict interpretation of the Environmental, Social and Governance (ESG), which lead banks and investment funds in the EU not to invest in the defence sector. Fifth, the support from dedicated public funding is fundamental to bridge the gap. The US and the UK have extensive programs supporting access to finance for innovative defence companies. French defence SMEs also benefit from public programs that offer tailored loans and equity support, a feature lacking in many other EU countries.

This first overview of the military expenditures and the technology investments (and of the existing funding) shows both progress and limitations in Europe's efforts to build a more integrated and capable defence innovation ecosystem and single defence market. Despite growing budgets and new instruments at the EU level,

such as the EDF, much of the investment remains fragmented and insufficient when compared to global counterparts. The importance of these recent initiatives lies not just in how much additional funding they bring, but in their ability to improve coordination, boost joint investment, and support shared technological development across EU countries.

DUAL USE TECHNOLOGIES: THE INVERTED FLOW AND THE CHANGING GEOPOLITICAL CONTEXT

The inversion of the innovation model

During most of the 20th century, the defence sector was the leader of technological innovation, with technology developed in defence labs often trickling into the civilian world. In the 1990s, however, due to a drastic decrease in defence budgets and the streaming of funds to commercial applications led by startup companies and Internet giants, the flow of innovation reversed direction. More and more, militaries depend on technologies developed initially for commercial markets and then spun into the defence sector. This entails different processes and priorities and working with non-traditional players. It also requires regular and meaningful dialogue between public and private sectors and increased investments specifically towards dual-use goods.

The shift from defence-led to commercially driven technological innovation has deep historical roots, shaped by changes in geopolitical priorities, industrial policies, and technological advancements. The Cold War era (1945–1990) further cemented the defence sector's role as a driver of technological innovation, particularly in the United States and the Soviet Union. Military and defence agencies led research efforts, with government-funded institutions and defence contractors at the forefront of technological development. Many of the key innovations of this period initially served military purposes before finding broader civilian applications. For instance, the Global Positioning System (GPS) was developed by the U.S. Department of Defense for military navigation before being opened to civilian use in the 1980s and 1990s. Similarly, the Internet originated from ARPANET, a U.S. military project in the 1960s, before becoming a backbone of global communication. Advances in semiconductors were also driven by military and space applications, with companies like Fairchild and Intel benefiting from defence contracts.

By 1960, the U.S. Department of Defense alone controlled 36% of global research and development (R&D) spending, effectively shaping the trajectory of technological evolution worldwide[50]. Defence-led R&D became a critical force behind innovation, with institutions such as the Defence Advanced Research Projects Agency (DARPA) playing a central role in fostering new technologies. This state-driven model of technological development not only advanced military capabilities but also facilitated the transfer of innovations to the civilian sector, reinforcing the broader economic and industrial landscape. The Cold War established a paradigm in which government investment in defence technologies shaped not only military power but also long-term economic and technological development across multiple sectors. In the 1960s, the U.S. federal government was the predominant source of R&D funding, with federal expenditures accounting for 66.8% of total U.S. R&D in 1964, while business contributions were at 30.8%. This trend has reversed in the past forty years. By 2022, the business sector funded 76% of total U.S. R&D, whereas the federal government's share had decreased to 18%[51].

This change took place because, from the end of the Cold War, defence budgets were significantly reduced, leading to a shift in the landscape of technological innovation. As government-funded defence projects declined, commercial technology firms began to play a more significant role in research and development (R&D). The global trend of deregulation and the rise of globalisation further accelerated this transformation, opening markets and providing opportunities for rapid innovation in civilian industries, particularly in computing, telecommunications, and software.
Key trends during this period include the rise of Silicon Valley

as a global innovation hub, with companies like Google, Apple, and Microsoft leading the charge in consumer technology. The shift from state-driven R&D to venture capital-backed startups became evident, as private investment increasingly replaced the large government defence contracts that had once dominated technological development. Alongside this, the emergence of dual-use technologies blurred the lines between military and commercial technological development. Over the past few decades, a significant shift has occurred, with a much larger share of capital now flowing into technologies primarily aimed at meeting civilian market demands.

This transformation is driven by three interrelated factors:

1. **The Decline of War Between States and Armed Conflicts Between Great Powers.** The end of the Cold War and the diminishing competition between Great Powers led to a gradual reduction in defence R&D funding. As the volume and intensity of state-level wars decreased, defence agencies reduced their focus and investment in military technologies. This shift in priorities opened the door for civilian markets to flourish, driving technological advancements in new sectors.
2. **The Rise of Startups and the Startup Ecosystem.** Startups became a key driver of innovation in the post-Cold War era. Their ability to adapt quickly, their small size, and high tolerance for risk allowed them to implement disruptive innovations. As the startup ecosystem grew, many of these companies evolved into the technology giants of today, dominating key areas of innovation by investing substantial amounts in R&D. Companies like Google, Apple, and Amazon now invest more in R&D than traditional defence contractors like Boeing and Lockheed Martin, with the R&D investments of these tech giants being more than triple those of the largest defence firms.
3. **The Emergence of Dual-Use Technologies and Commercial Solutions.** In this new landscape, dual-use technologies have become increasingly common. Innovations such as artificial intelligence (AI), cybersecurity, and cloud computing, which were once solely the domain of military R&D, are now primarily developed by private tech firms. Tesla, Google, and Amazon, for example, invest more in AI than most defence agencies, with these technologies having broad applications across both civilian and defence sectors. The shift has forced defence agencies to adapt commercial solutions rather than lead their development.

The militarisation of emerging technologies

The growing integration of civilian-developed technologies into military applications has significantly altered the defence landscape. Advances in Artificial Intelligence (AI), autonomous systems, space technologies, and telecommunications - originally designed for commercial purposes - are now being repurposed for military use at an unprecedented pace. This trend, known as the militarisation of emerging technologies, challenges traditional distinctions between civilian and defence sectors and raises concerns about governance, regulation, and geopolitical stability.

One of the most striking examples of this shift is the adaptation of unmanned aerial vehicles (UAVs), or drones, for military operations. Initially developed for commercial and recreational use, drones have become essential assets in modern warfare[52]. The widespread availability of commercial drone technology has enabled state and non-state actors to deploy low-cost, high-impact aerial systems for surveillance, reconnaissance, and direct attacks. To make some concrete recent examples:

- The Turkish Bayraktar TB2, a drone developed for reconnaissance, has been extensively used in conflicts such as the Nagorno-Karabakh war (2020) and the Russia-Ukraine war (2022–present). Ukraine's military has effectively employed these drones against Russian armoured vehicles, demonstrating how commercial drone technology can shift the balance on the battlefield[53].
- In the Middle East, groups such as Hezbollah and the Houthis have modified civilian drones to carry explosives, conducting attacks on infrastructure and military targets.

- The United States and China have invested heavily in developing loyal wingman drones, such as the XQ-58 Valkyrie (U.S.) and FH-97 (China), which leverage AI for autonomous operations alongside fighter jets.
- Operation Spiderweb[54] represented Ukraine's coordinated use of small, long-range drones to attack Russian military aircraft deep inside Russian territory, including airfields hundreds of kilometres from the border. This innovative drone campaign demonstrates how low-cost, distributed technologies can disrupt traditional air superiority and reshape modern warfare tactics.

Satellite technology, initially developed for civilian communication and navigation, has become a critical enabler of military operations. The fusion of commercial space technology with defence capabilities highlights the increasing overlap between the two sectors:

- Starlink, the satellite Internet constellation developed by SpaceX, was originally intended to provide global broadband coverage, particularly to underserved regions. However, since the outbreak of the Russia-Ukraine war, Starlink has been used by Ukrainian forces for secure battlefield communications and drone coordination, demonstrating how commercial space infrastructure can become a strategic asset in warfare[55].
- In response to the growing militarization of space, China has ramped up its dual-use satellite programs, integrating commercial Earth observation systems into military intelligence operations. The Gaofen satellite series, developed for civilian applications such as disaster monitoring and environmental protection, is also used for high-resolution reconnaissance.
- The United States have strengthened collaboration between SpaceX, Amazon's Kuiper, and the Department of Defence to ensure access to secure satellite communications and real-time intelligence. The Pentagon's Blackjack program[56], for instance, aims to leverage commercial small satellites for defence applications.

AI-driven technologies initially developed for commercial automation, data processing, and cybersecurity are now at the forefront of modern military strategies. Governments and defence contractors are rapidly integrating AI into decision-making, autonomous systems, and cyber warfare operations.

- AI-powered target recognition systems, such as Project Maven[57], leverage machine learning to analyse vast amounts of video and sensor data, enhancing battlefield intelligence for the U.S. military.
- Autonomous weapons, including AI-guided missile systems and unmanned ground vehicles, are being developed by defence firms such as Lockheed Martin and China's Norinco, raising concerns about lethal autonomous weapon systems (LAWS) and the potential for AI-driven conflicts.
- The use of AI in cyber warfare has expanded, with algorithms designed for cybersecurity threat detection now being repurposed for offensive cyber operations, including disinformation campaigns, electronic warfare, and AI-enhanced hacking strategies.

A particular mention should also go to secure telecommunication networks in particular 5G and in the future 6G that have increasing potential applications in the military[58]. Using the 3GPP standards 5G applications are being used in unmanned ground vehicles, local networks, maritime communication, aircraft, terrestrial trunked radio replacement[59]. Combining mobile 5G networks with satellite communication brings further potential benefits and use scenarios that are being actively researched in the context of 5G advanced and 6G. Combining LTE with satellite backhaul (e.g., Starlink) enhances network resilience. Mobile network-enabled drones are now increasingly used both by Ukraine and Russia in the war.

The increasing adaptation of civilian technologies for military purposes underscores the blurring of boundaries between commercial and defence sectors. As states compete for technological supremacy, the acceleration of dual-use applications poses new governance challenges and risks exacerbating global

security tensions. Addressing these challenges will require a coordinated regulatory framework, increased transparency in military AI applications, and stronger safeguards to prevent the misuse of emerging technologies in conflict scenarios. Particular attention should go to ethical considerations in dual-use innovation, particularly for AI and autonomous systems. Ethical and legal safeguards aligned with humanitarian law should be incorporated as part of the governance of dual-use technologies. Such safeguards should state what these technology can and cannot do, with the aim of avoiding potential for misuse, civilian harm, and escalation of conflict.

The role of venture capital and startups

The growing role of private companies and venture capital in dual-use research and development (R&D) has transformed the landscape of technological innovation, making commercial actors key players in national security and defence. Unlike in the past, when military agencies led the development of cutting-edge technologies, today's most critical advancements are increasingly driven by the private sector. Tech giants and startups alike are now at the forefront of dual-use innovation. Companies such as SpaceX, Palantir, Anduril, and Microsoft have developed technologies that serve both commercial and defence markets, often outpacing government-led R&D. In Europe, firms like Airbus, Thales, and Leonardo play a crucial role in defence innovation, while emerging AI and cybersecurity startups are increasingly engaged in dual-use applications.

There is a growing demand from governments for innovative defence technologies to which defence start-up and the Venture Capitalists (VC) increasingly supporting them are responding, particularly in the United States and to a lesser extent in Europe [60][61]. National security agencies and ministries increasingly seek to source technologies from companies beyond the traditional defence sector.

While not a recent development, this shift can be observed in three separate waves of defence tech start-ups over the last 20 years[62] (see figure below). In the US, the first wave of defence tech start-ups in the early 2000s included companies like SpaceX and Palantir, which created technology for government agencies outside the Department of Defense. A second wave emerged in the mid-to-late 2010s with companies like Anduril (2017) and ShieldAI, using commercial technology for defence applications. Today, a third wave is rising, with a larger group of start-ups and nontraditional companies driving innovation, attracting significant venture capital, and scaling up[62]. These start-ups are often well-equipped to address critical national security needs, complementing the traditional defence industry.

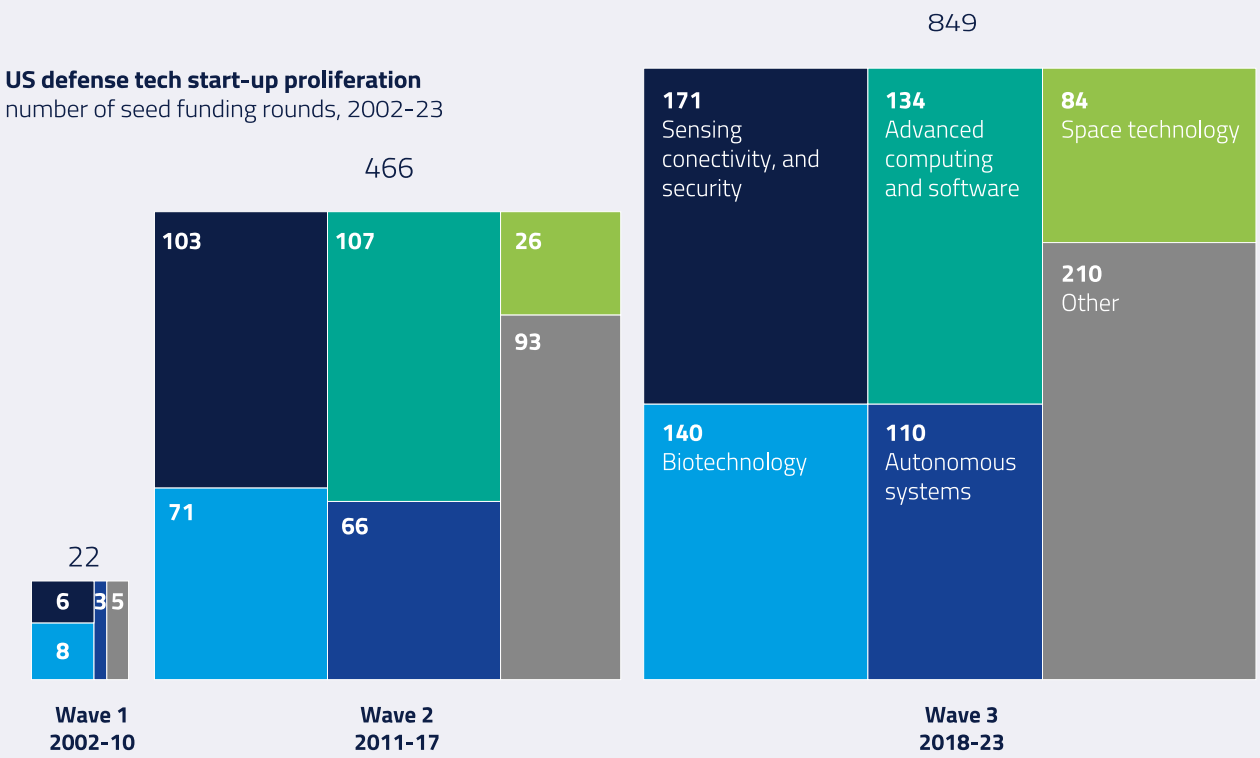

Figure 3 US defence tech start-up proliferation, Source: McKinsey, 2024

The European defence tech start-up ecosystem lags about five years behind its U.S. counterpart in terms of maturity. European start-ups often face bureaucratic hurdles and a lack of coordinated efforts across EU Member States. These barriers hinder their ability to scale quickly and attract significant investment, slowing the development of innovative defence solutions. Despite these barriers, a report on the state of Defence, Security and Resilience in Europe published in February 2025 by the Nato Innovation Fund and research group Dealroom[63], reveals a record-breaking year for investing in this segment. This highlights the critical role that the sector is playing in maintaining Europe's technological edge and sovereignty. In particular, VC funding in the sector reached $5.2 billion in 2024, which is up nearly 5x in the last six years. In Europe, Germany and the UK are emerging as regional leaders. In particular, Munich emerged as Europe's top hub, attracting almost $1 billion in funding in 2024, followed by Oxford in the UK and Paris in France.

The increasing interest of VC in the sector is even more exceptional if considered in the broader context of VC funding trends in European startups. With an increase of 30% in the last two years, the deep tech defence segment has outperformed the overall VC market, which witnessed a 45 percent decline in the same period of time[64] (see figure below).

This growing reliance on private funding introduces serious governance challenges:

1. **National Security vs. Market Incentives** – Private investors prioritize profitability and scalability, which may not always align with long-term defence needs[65]. Some

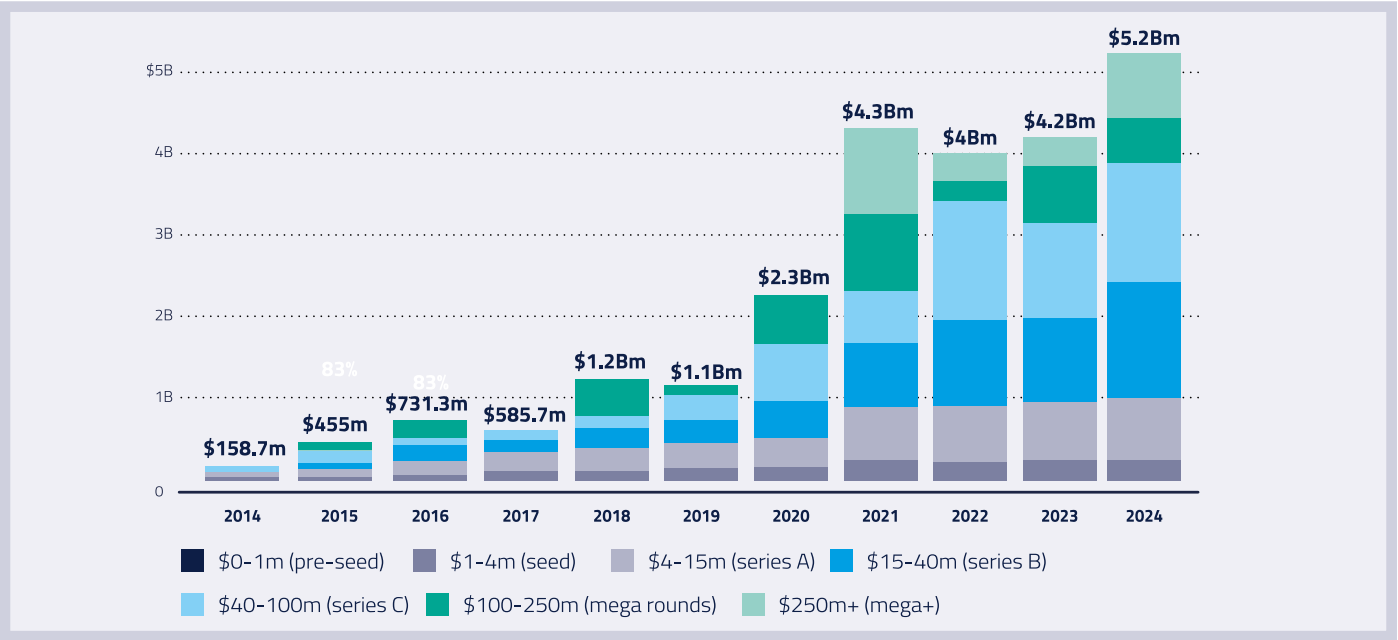

Figure 4 VC funding in European defence tech startups, Source: Dealroom.co

Vertical	% last 12 months growth	last 24 months	2024	2023	2022	2021	2020	2019
Total VC	**-11%**	**-45%**	**$54B**	**$60B**	**$98B**	**$116B**	**$48B**	**$47**
Robotics	15%	15%	$2B	$1B	$2B	$2B	$644M	$838M
Enterprise software	31%	-48%	$10B	$7B	$19B	$17B	$7B	$6B
Defense security and resilience	**24%**	**30%**	**$5B**	**$4B**	**$4B**	**$4B**	**$2B**	**$1B**
Health	12%	-13%	$11B	$10B	$12B	$18B	$10B	$8B
Fintech	8%	-64%	$9B	$8B	$24B	$29B	$11B	$12B
Marketing	4%	-59%	$2B	$2B	$6B	$7B	$3B	$3B
Rest of Deep tech*	-24%	-32%	$10B	$13B	$15B	$14B	$7B	$7B
Food	-26%	-49%	$4B	$5B	$7B	$12B	$4B	$3B
Transportation	-32%	-52%	$6B	$9B	$13B	$13B	$6B	$6B
Semiconductors	-38%	-1%	$1B	$2B	$1B	$1B	$899M	$496M
Energy	-39%	-30%	$9B	$16B	$13B	$10B	$4B	$3B
Real Estate	-49%	-62%	$1B	$3B	$3B	$3B	$2B	$2B

Figure 5 Comparison of VC funding by selected sectors in Europe, Source: Dealroom.co

critical technologies may be underfunded if they lack clear commercial applications.

2. **State Dependence on Private Firms** – Governments risk losing control over essential technologies and infrastructure. For instance, Starlink's role in Ukraine has raised concerns about the implications of relying on a private company for critical military communications.
3. **Fragmentation of European Defence Efforts** – Unlike the U.S., where defence procurement is centralized, Europe's fragmented defence market makes it difficult for startups to scale across multiple national jurisdictions, limiting their ability to secure defence contracts.

Furthermore, there are some structural problems behind the dual-use strategy. Despite its intended benefits, it has introduced inefficiencies in defence acquisition. By requiring companies to first establish commercial viability before engaging with military applications, this approach creates delays in adopting cutting-edge technologies for defence purposes. In contrast, China's civil-military fusion system ensures rapid integration of emerging technologies, giving it a competitive advantage. Instead of reforming slow and bureaucratic procurement processes, many defence agencies encourage private sector adaptation, shifting the burden of speed and innovation onto startups while maintaining outdated acquisition cycles. In the European context, this issue is compounded by the lack of a cohesive defence industrial policy. While the EU has taken steps toward greater defence cooperation through PESCO (Permanent Structured Cooperation) and the EDF, significant barriers remain in streamlining procurement and scaling dual-use innovations across member states. Without more agile funding mechanisms and faster

procurement processes, European defence actors may struggle to keep pace with global competitors.

Strategic autonomy, technological sovereignty and dual-use export control

In recent years, the global landscape has undergone profound transformations. Key factors such as rapid advancements in technological capabilities - most notably China's expanding scientific influence -, rising geopolitical tensions and conflicts, and intensifying competition between different political and value systems have increased concerns. As observed by Edler et al.[66]: "The globalist assumptions of the post-Cold War era - that reliable, mutually beneficial agreements could be reached with all nations, regardless of ideology - have been shattered. Recent geopolitical and geo-economic developments have brought a previously less visible, largely political, risk dimension to the forefront."

Against this backdrop, concepts such as strategic autonomy and technological sovereignty have gained prominence in policy debates across Europe and beyond[67]. These discussions reflect growing apprehensions over Europe's complex dependencies and the vulnerabilities they entail. They are spread across various domains, from military and digital technologies, where Europe relies heavily on the United States, to energy security, which was strongly exposed by Europe's dependence on Russian fossil fuels[68]. The latter became particularly problematic following Russia's invasion of Ukraine in 2022, prompting urgent efforts to diversify energy sources through different measures.

Additionally, Europe's economic and industrial reliance on China, exemplified by the solar panel industry but even more critically linked to rare earth materials, has drawn increased scrutiny. The COVID-19 pandemic and the resulting supply chain disruptions further underscored these vulnerabilities, particularly in sectors deemed strategically vital. Compared to 2020-2021, Europe's dependence on China, especially concerning critical material supply chains, is now more openly debated, even though significant regional disparities remain in how these dependencies are recognised and addressed[69]. These evolving challenges have further intensified discussions on technological sovereignty and strategic autonomy.

In this new geopolitical context, there are growing concerns about the resurgence of interventionist and protectionist policies, often accompanied by increasing isolationism. Such policies risk disrupting global trade flows and undermining the interdependent production networks that have historically benefited Europe and other regions. The concepts of "strategic autonomy" and "technological sovereignty" were initially introduced in 2013 within the context of defence and security policies, but they have since expanded into other policy domains, including trade, industrial policy, and innovation policy. Policy measures aimed at strengthening technological sovereignty and strategic autonomy generally fall into three broad categories: protection, promotion, and partnering[70].

- **Protection Measures:** According to the OECD, protective measures—such as export controls, foreign direct investment (FDI) screening, restricted technology lists, and research security policies—are expected to drive a decoupling from China's technology and, potentially, scientific ecosystems. This could weaken international research collaboration and reduce technological and scientific exchanges. Trade and investment restrictions may also negatively impact technology-intensive companies.
- **Promotion Measures:** These measures focus on strengthening domestic industrial capacity and reducing reliance on foreign suppliers, thereby supporting scientific and innovation activities. They often involve targeted industrial policies, increased funding for research and development (R&D), and incentives for local technological advancements. However, promotion measures can also have unintended consequences. One key risk is triggering a subsidy race, where countries compete to attract high-tech industries through financial incentives. This could undermine international cooperation and lead to inefficiencies.

- **Partnering Measures:** These measures aim to diversify international partnerships and reduce excessive dependence on specific regions. Often integrated into broader "recoupling" strategies, they focus on securing resilient supply chains, fostering cross-border collaboration in science and technology, and strengthening capabilities. Moreover, these measures play a crucial role in promoting sustainability values and driving global investments in research and innovation, particularly in middle- and low-income economies.

A key challenge global players confront today is how to best exercise regulatory and trade controls over sensitive dual-use technologies. Limiting access to technologies is essential for maintaining strategic technological advantages over competitor players. However, as the nature of military technology development has evolved, governments have had to rethink export control strategies aimed at limiting access to critical technologies. During the Cold War, these controls primarily targeted military hardware, while most commercial products remained largely unrestricted. With the end of the Cold War, 33 countries approved in 1996 the first global multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies called the Wassenaar Arrangement (WA)[71]. The WA was designed to promote transparency, exchange of views and information and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. It complements and reinforces, without duplication, the existing regimes for non-proliferation of weapons of mass destruction and their delivery systems, by focusing on the threats to international and regional peace and security which may arise from transfers of armaments and sensitive dual-use goods and technologies where the risks are judged greatest.

Today, governments need to reassess the role of commercial technologies in enhancing competitor's military capabilities and develop targeted strategies to limit access where necessary[72]. Effectively managing these trade-offs requires active engagement with the private sector. Without industry buy-in, resistance from commercial actors can hinder the effectiveness of restrictions and risk politicising the issue. To succeed in limiting access to critical technologies to trusted partners, governments must actively involve, incentivise, and monitor industry stakeholders. Market operators have deep expertise that the Ministries of Defence and Trade must leverage to ensure technology controls are both effective and precisely targeted. The objective is to minimise economic costs while maximizing strategic impact. Industry engagement also helps prevent government-imposed restrictions from triggering supply chain disruptions that could slow technological innovation.

One of the most relevant examples of how the new global landscape is entangled with the regulatory and trade controls of sensitive dual-use technologies is provided by the semiconductor market, which has become a focal point in the contest for technological dominance. Semiconductors are essential for consumer electronics, advanced artificial intelligence (AI) systems, as well as military applications. Countries that lead in semiconductor design and manufacturing hold significant commercial and strategic leverage. Recognising this, China has made semiconductor self-sufficiency a national priority, investing massive resources into its domestic industry to reduce reliance on Western suppliers. However, this ambition has been met with increasing restrictions from around the world, aimed at preventing China from gaining access to cutting-edge chipmaking technologies. Most notably, the U.S. Government has taken aggressive steps to reduce China's semiconductor capabilities. The export controls imposed severe restrictions on China's ability to access U.S.-developed AI chips and semiconductor manufacturing equipment[73]. These measures aim to slow China's ability to develop high-performance chips essential for AI applications, including military and intelligence uses. Given that China remains dependent on advanced machinery from the U.S., the Netherlands, and Japan, these restrictions have significantly hindered its ability to scale domestic production.

However, these export controls have not come without controversy and criticism from the industry. European and Asian semiconductor companies, as well as U.S. firms, have expressed concern over the impact of these restrictions on their business operations. China is one of the largest markets for semiconductor products and losing access to this market risks significant revenue losses for Western firms. Companies in the Netherlands, Japan, and the EU have pushed back on additional export restrictions, particularly those limiting service and maintenance of previously sold chipmaking equipment. The debate highlights the broader tension between national security imperatives and the commercial interests of private-sector actors. As the semiconductor case illustrates, strategic technology controls are becoming more complex in an era where economic and security interests are deeply intertwined. Policymakers will need to navigate these trade-offs carefully, ensuring that restrictions do not accidentally weaken the very industries they seek to protect.

EU DEFENCE POLICY: RECENT INITIATIVES, R&D FUNDING, AND EXPORT CONTROL

Recent EU initiatives: the new centrality of defence policy

Since the Russian invasion of Ukraine in February 2022, the EU defence policy has increasingly recognised the economic security risks emerging from increasing geopolitical tensions, geo-economic fragmentation, and profound technological shifts. The EU immediately reached a collective decision that the security and defence component, which had historically carried less weight compared to other EU policies and had largely been rooted at the national level, should now gain prominence.

EU Heads of State or Government met in Versailles on 11 March 2022[74] and made the commitment to bolster European defence capabilities in support of Ukraine. They agreed to: a) increase defence expenditures; b) step up cooperation through joint projects; c) close shortfalls and meet capability objectives; d) boost innovation including through civil-military synergies; and e) strengthen and develop European defence industry, including SMEs. At the Versailles Summit, EU leaders agreed to invest 'more and better in defence capabilities and innovative technologies'. The meeting was followed by the adoption in March 2022 by the Council of the Strategic Compass on Security and Defence[75]. The Strategic Compass presented a plan of action to strengthen the EU's security and defence policy by 2030 and enhance the EU's strategic autonomy. The overall ambition of the plan is to develop "full spectrum forces that are agile and mobile, interoperable, technologically advanced, energy efficient and resilient". On 20 June 2023, the European Commission and the High Representative for Foreign and Security Policy adopted a Joint Communication on a European Economic Security Strategy[76]. This strategy provides a framework for assessing and addressing risks to EU economic security while ensuring that the EU remains an open and attractive destination for business and investment. The strategy identifies four key risk categories: risks to the resilience of supply chains; risks to the physical and cyber-security of critical infrastructure; risks for technology security and technology leakage; and risks of weaponisation of economic dependencies or economic coercion. To address these risks, the strategy is built on three pillars: Promoting the EU's competitiveness and growth, Protecting the EU's economic security, and Strengthening partnerships and cooperation worldwide.

About one year later, in March 2024, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy adopted the European Defence Industrial Strategy (EDIS)[77], which highlighted the "return of high intensity warfare in Europe" and the consequent need for the European defence industry to mass produce "a large set of defence equipment such as ammunition, drones, air defence missiles and systems, deep strike and intelligence, surveillance and reconnaissance capabilities, as well as the ability to ensure its swift and sufficient availability". The EDIS calls for investing 'more, better, and European'. The EDIS also highlighted that the EU and its Member States are faced "with the contestation of Europe's access to strategic domains such as the

space, cyber, air and maritime domains". In support of the EDIS, a regulation for the establishment of European defence industry programme (EDIP)[78] to ensure timely availability and supply of defence products was proposed. The proposal foresees allocating €1.5 billion to the EDIP for 2025-2027. EDIP aims at establishing the conditions and criteria for Member States to form consortia that qualify as a European Defence Capability Consortium (EDCC) that will jointly procure, for the use of participating Member States, defence capabilities that are developed in a collaborative way within the EU and would benefit from a VAT exemption. This new vehicle would complement existing related options under the umbrella of the EDA, while it could also serve projects in the PESCO framework.

This process of developing EU defence policies and initiatives culminated in March 2025, when first the Re-Arm EU plan was presented and later it was fleshed out in the White Paper[79]. The rationale for Re-Arm Europe is two-fold. On the one hand, the deteriorating geopolitical context is described as posing several threats to Europe's security and strategic autonomy. On the other hand, the current gaps in the European Defence Technological and Industrial Base (EDTIB) deriving from decades of underinvestment are identified. The European defence industry cannot produce defence systems and equipment in the quantities and speed that are currently needed and is fragmented 'with dominant national players catering mostly to domestic markets'. Both call for urgent action and a surge in defence spending to reach readiness in 2030 in broadly defined defence capabilities. It is important to stress that, besides the gap in traditional defence production capabilities, Re-Arm Europe also stress the technological dimension and dual-use technologies. The White Paper states that "Geopolitical rivalries have not only led to a new arms race but have also provoked a global technology race. Technology will be the main feature of competition in the new geopolitical environment. A handful of critical and foundational technologies like AI, quantum, biotech, robotics, and hypersonic are key inputs for both long term economic growth, and military pre-eminence. Boosting innovation is key for this. As such, technology diffusion for commercial purposes must be reconciled with more rigid technology ecosystems to advance national security objectives. The EU's strategic competitors are heavily investing in this area"[80]. It recognises that: a) some technologies can produce defence superiority as they are changing the nature of warfare; and b) in such technologies the distinction between civilian and defence is blurred and, thus, "innovative civilian startups and relevant R&I results can play a crucial role in developing cutting-edge solutions that can significantly enhance military capabilities and improve operational readiness"[81]. European defence should invest in disruptive technological innovations to fill the current gap to 'regain edge and prevent being technologically dependent'[82]. Accordingly, the White Paper announces that the EU will present a European Armament Technological Roadmap to leverage "dual use advanced technological capabilities at EU, national and private level. In an initial phase the EU will focus on AI and quantum. The Commission will also ensure that the European Innovation Council and the planned TechEU Scale-up Fund will invest in dual-use technologies"[83]. In concrete, the Re-Arm EU plan foresees a surge in spending through five mechanisms:

1. **A new financial instrument:** Security and Action for Europe (SAFE). This would provide loans backed by the EU budget for up to EUR 150 billion. SAFE will support the European defence industry through common procurements involving at least two countries, out of which one shall be a Member State receiving SAFE financial assistance and the other may be another Member State, an EFTA State, member of the EEA or Ukraine.
2. **Activation of the National Escape Clause of the Stability and Growth Pact.** Flexibility to the stability and growth path is introduced allowing Member States to invest up to 1.5% of GDP for defence expenditure outside of the pact limits. This should allow defence investment to increase of up to EUR 800 billion in the next four years.
3. **Making existing EU instruments to allow greater defence investments.** In the short term, the EU can do more to

support the urgent need to increase European defence investments with the EU budget such as, for instance, from cohesion policy funds.

4. **Contributions from the European Investment Bank (EIB).** The EIB should play a key role in funding European Defence, by introducing changes that would lower current limitations and widen the scope of its defence-related funding. The EIB allegedly plans to increase its investment to up to EUR 2 billion and fund projects such as drones, space, cybersecurity, quantum technologies, military facilities, and civil protection[84].
5. **Mobilising private capital.** Public investment will not be sufficient, as European companies (both SMEs and mid-caps) need to have better access to capital to bring their solutions to industrial scale and to drive the industrial ramp-up that Europe needs. It is anticipated that the initiative Savings and Investment Union should channel resources to EU priorities, including the defence sector. To this purpose the Commission will clarify the EU's Sustainable Finance Disclosures Regulation (SFDR), as to possible limitations to financing defence activities.

The roadmap for 2025 includes several initiatives, the most noteworthy of which are: a) Member States are expected to request the activation of the 'Escape Clause'; b) the Council should adopt the proposed draft Regulation on Security and Action for Europe (SAFE); c) the co-legislators should adopt the European Defence Industry Programme (EDIP) before the Summer 2025, including its Ukraine Support Instrument (USI); d) the Commission will present, by June 2025, a Defence Omnibus Simplification proposal; e) the EU will present a European Armament Technological Roadmap on investment into dual-use advanced technological capabilities in 2025.

R&D in dual use technologies: from separation to convergence

Dual-use technologies represent both a challenge and an opportunity for modern economies. On the one hand, civilian innovations drive economic growth and should be actively supported by both private and public actors through R&D investments. On the other hand, the potential military applications of these innovations pose security risks, as the export of such goods could support states that violate human rights or international treaties. As a result, governments face the ongoing challenge of balancing regulation - through measures such as export controls and restrictions in public investment programs - with the need to incentivise technological development. In recent years, Europe has increasingly prioritised economic considerations in its approach to dual-use technologies[85]. This shift reflects not only a commitment to fostering a competitive dual-use industry but also a strategic effort to strengthen Europe's defence capabilities in response to evolving geopolitical dynamics. The EU's stance highlights the intersection of economic growth, security imperatives, and the broader objective of achieving greater strategic autonomy.

Historically, the EU has maintained a clear separation between civilian and military research and innovation. This principle, grounded in political and ethical considerations, resulted in parallel ecosystems with distinct stakeholder communities, objectives, regulatory frameworks, and funding instruments. Horizon Europe, the EU's flagship research and innovation programme, has supported R&D with an exclusive focus on civil applications. Defence stakeholders were not automatically excluded, but any participation had to remain within the scope of civil uses, and proposals explicitly including defence applications were ineligible. Meanwhile, the European Defence Fund (EDF) was created to support defence-specific R&D, with a strict focus on military capability development, even though many EDF projects inherently had civilian spillovers.

However, the new geopolitical context marked by increased instability, technological rivalry, and Russian invasion of Ukraine has profoundly altered this landscape. Even before the 2025 White Paper "Readiness 2030," European leaders recognised that increased investment in dual-use technologies could enhance both the EU's competitiveness and its defence capabilities. The

2024 Report "Science, Research and Innovation Performance of the EU (SRIP)" published by the European Commission highlighted that the EU should harness the untapped potential of dual-use technologies in areas such as artificial intelligence, quantum, biotechnology, information technology and robotics[86]. In the same year, the European Commission introduced initiatives targeting key regulatory levers to maximise these opportunities, including a White Paper encouraging discussions on how to better support research and development in technologies with dual-use potential[87]. This initiative aimed to overcome the longstanding division between civil and defence R&D. As described in the previous sections, the major change in the dynamics of defence innovation, with more groundbreaking technologies emerging from the private sector, rather than the defence industry, calls for a new approach to European R&D policy.

Yet, the EU funding landscape struggled to adapt. In 2018, the European Parliament and the Council agreed that research and innovation activities should be maintained separately. Horizon Europe, the EU's flagship research and innovation program, supports R&D with an exclusive focus on civil applications. While projects must be strictly civilian, many research areas—such as digital technologies, cybersecurity, energy, mobility, health, materials, and space—have potential dual-use applications. Meanwhile, the EDF focused solely on defence-related R&D, although many projects produced innovations with broader civilian relevance. Limiting military-civilian fusion has proven too restrictive for fostering innovation and industrial development. As Schwaag Serger et al. note[88]: "DARPA has allowed the US to drive disruptive innovation and technology development that meet both national defence needs and benefit US economic growth (through commercial applications). China has pursued civil-military fusion for many years. For historical reasons, Europe has sought to keep civilian and military research and innovation systems apart."

Acknowledging this limitation, the Commission launched a series of actions since 2021 to improve synergies between EU programmes and promote an EU-wide approach for critical technologies by making best use of EU R&D programmes[89]. The 2021 Action Plan on Synergies between civil, defence, and space industries outlined key steps, including the creation of a dual-use innovation incubator and early screening of research proposals to identify broader application potential. The European Innovation Council (EIC) and the European Defence Innovation Scheme (EUDIS) have also been instrumental in providing targeted support to SMEs, start-ups, and non-traditional defence actors.

The 2024 White Paper "On options for enhancing support for research and development involving technologies with dual-use potential"[90] presented three possible scenarios:

1. **Scenario 1:** Incremental Improvements. A cautious approach would refine existing measures, like spin-in calls under EDF and InvestEU support for dual-use firms. This expands opportunities while minimizing disruption but may limit deeper civil-defence integration.
2. **Scenario 2:** Dual-Use Research in FP10. The Commission proposes allowing dual-use technologies in the new Framework Research Programme (FP10), removing the 'civilian-only' rule in select areas. Defence projects could integrate with EU-funded research, with EDF providing follow-up funding. This boosts strategic autonomy but raises concerns over ethics and participation rules.
3. **Scenario 3:** New Dual-Use Fund. A stand-alone funding instrument could target dual-use R&D but risks adding complexity and duplicating existing programmes. While supporting commercialisation, it raises concerns over coordination and efficiency.

This shift in thinking was reinforced by the Draghi Report[91], which recommended increased and more coordinated R&D funding focused on common strategic priorities. Indeed, according to the Report, the European defence industry faces challenges beyond lower defence spending, as it also lacks a strong focus on technological development. Despite being globally competitive,

with an annual turnover of €135 billion in 2022 and strong exports, the defence sector struggles with a capacity gap on two fronts. First, an overall low overall demand, as aggregate EU defence spending is about one-third that of the US. Second, a limited focus on innovation, as defence is a highly technological industry that relies on disruptive innovation, requiring massive R&D investment to maintain strategic parity.

The Draghi Report highlights the urgent need for increased defence investment and greater EU-level cooperation in defence R&D. The sector faces massive investment needs, and while deeper EU capital markets will help, innovative defence SMEs require additional support. Measures suggested in the Report include revising the EIB Group's lending policies on defence and clarifying ESG frameworks for financing defence products. Currently, the EU invests just €1 billion annually in defence R&D, with most funding coming from Member States. However, emerging technologies—such as drones, hypersonic missiles, directed-energy weapons, AI in defence, and seabed and space warfare—demand a pan-European approach. No single country can independently finance, develop, and sustain leadership in these fields. To address this, the Report proposes new dual-use programmes and European Defence Projects of Common Interest to structure industrial cooperation, maximize spillover benefits to other sectors, and strengthen Europe's technological leadership in defence.

The publication of the Re-Arm EU plan and the proposal for "Readiness 2030" have marked a turning point. The Commission's new proposal introduces targeted amendments to existing EU funding programmes, aimed at accelerating and coordinating investments in Europe's defence technological and industrial base (EDTIB). This includes a Regulation to stimulate defence-related investments under the EU budget and enhance strategic readiness.

A central element of this shift is the Strategic Technologies for Europe Platform (STEP), whose scope is now broadened to cover defence-related technologies and products, particularly those identified as priority capabilities in the 2025 White Paper. Selected projects under Horizon Europe, the EDF, and the Digital Europe Programme will be awarded the "STEP Seal," enabling faster and more flexible funding. STEP will also facilitate the use of cohesion policy funds (ERDF, CF) to support critical technologies for defence, creating a new financial architecture for dual-use innovation.
Further, the Horizon Europe Regulation now explicitly supports the inclusion of dual-use and defence-related innovations within the EIC. This expansion aims to foster a dynamic innovation ecosystem where start-ups can accelerate the development and deployment of cutting-edge technologies, especially in areas like AI and cybersecurity. The Digital Europe Programme (DEP) will also expand to include dual-use applications. This includes the development of AI Gigafactories—essential for scaling advanced technologies for both civilian and military use. Additionally, the Regulation introduces flexibility in the use of cohesion policy funds to reinforce the EU's defence industry. Notably, it includes a "landing clause" allowing Member States to voluntarily transfer resources from cohesion policy programmes to the EDF or the Act in Support of Ammunition Production (ASAP), whose duration has now been extended to 31 December 2026. Lastly, the Connecting Europe Facility (CEF) has been updated to enhance support for military mobility and dual-use digital infrastructure. This includes enabling Member States to channel cohesion funds into dual-use transport infrastructure projects and expanding the CEF Digital Programme to support capacities in AI, cloud, and 5G relevant to both civil and defence needs. Together, these developments signal a profound shift in EU policy—from separation to convergence—between civil and defence R&D. The narrative of "keeping things apart" is being replaced by a coordinated, strategic effort to leverage Europe's full innovation potential in an increasingly contested global environment.

Very recently, the European Commission has published the Communication on the EU Startup and Scaleup Strategy[92] and the proposal for the establishment of the European Competitiveness

Fund (ECF)[93], both of which could positively support dual-use and defence innovation. In the Startup and Scaleup Strategy emphasis is place on the need of regulation simplification and there is a special mention that: "The Commission will leverage and reinforce existing instruments and develop new instruments to invest in European security and defence startups and scaleups, in line with the White Paper on Defence and based on the upcoming Omnibus Defence Simplification Package"[94]. The proposal on the ECF has a special focus on the defence sector and on dual-use technologies.

Export control of dual use technologies

Dual-use items are subject to stringent export controls in the European Union, which goes beyond the global multilateral arrangement on export controls (Wassenaar Arrangement) mentioned before in the report. The EU regulation of dual-use exports is essential for maintaining security, ensuring compliance with international obligations, and balancing trade interests. The risks associated with dual-use items include their potential use in World Mass Destruction programs, military applications, and human rights violations. Consequently, the EU has developed a robust export control system to mitigate these threats while facilitating legitimate trade.

The EU has long recognised the need to modernise its export control framework in response to evolving security challenges, technological advancements, and shifts in global trade patterns. Following a 2014 communication outlining potential revisions, the European Commission proposed an overhaul of the export control system in 2016. This culminated in the adoption of Regulation (EU) 2021/821 on 20 May 2021, which strengthened the EU's ability to address emerging security risks effectively. The revised regulation introduced a more dynamic approach to export controls, reinforcing coordination between EU Member States and improving mechanisms to assess and mitigate security risks. It also enhanced transparency and engagement with stakeholders, including industry representatives, academia, and civil society, to ensure a balanced approach between security and economic interests.

Although dual-use items can be traded freely within the EU, certain sensitive items remain subject to prior authorization, as outlined in Annex IV of the regulation. Additionally, Member States retain the right to impose additional controls based on national security and human rights considerations. The dynamic nature of security threats, scientific advancements, and geopolitical developments necessitates continuous updates to the EU's export control framework. The European Commission maintains an ongoing dialogue with stakeholders to refine the system and ensure its effectiveness. In January 2024, the Commission published a White Paper on Export Controls, addressing the growing complexity of global trade and security risks. The paper emphasizes the need for adaptive controls, enhanced enforcement mechanisms, and stronger cooperation with international partners to safeguard the EU's security interests.

International trade in dual-use items plays a crucial role in Europe's economy. According to the latest report mandated by the modernised EU Export Control Regulation, dual-use exports are under increasing scrutiny by both the EU and its Member States[95]. In 2022, Member States authorised dual-use exports worth €57.3 billion, accounting for 2% of extra-EU exports of goods. In the same year, 831 export applications were denied due to security risks, representing a total value of €0.98 billion, or approximately 0.03% of extra-EU exports. These figures mark a significant increase from 2021, when authorised exports totalled €38.5 billion (1.8% of extra-EU exports), and 568 denials were issued, amounting to 0.01% of extra-EU exports. These figures highlight the significant socioeconomic impact of the dual-use sector and the importance of maintaining its global competitiveness to support Europe's long-term growth objectives.

However, recent trends in export controls suggest a shift toward tighter regulation. The latest EU report provides, for the first time, extensive licensing data that enhances transparency on how export controls are applied, and the risks associated with sensitive exports in the current geopolitical context. This

tightening of export controls comes amid growing concerns about Europe's competitive position. The United States' reform of its dual-use export regime in 2009 aimed at improving its global competitiveness, prompting similar discussions within the EU. The European Commission subsequently launched a review of its dual-use policies, responding to industry calls for a more flexible approach, particularly in light of competition from China and India. Striking the right balance remains crucial to ensuring that efforts to enhance global competitiveness do not compromise security commitments[96].

SCENARIOS

MAIN AREAS OF UNCERTAINTIES

The analysis presented so far shows that there is wide awareness and consensus on the fact that dual-use technologies are strategic assets essential for both economic resilience and military readiness. As Europe faces intensifying geopolitical competition and rapid technological change, the effective development of dual-use technologies with both civilian and military applications will be critical for its strategic autonomy and technological sovereignty. Furthermore, establishing a strong position in dual-use technologies is also essential if the EU wants to have a say on their regulation and governance, namely on the definition of what is a responsible an ethical use of such technologies in defence applications. This means defining what digital technologies can and cannot do when used to steer defence applications.

These technologies include Artificial Intelligence (AI), autonomous systems, sensing, quantum computing, Internet of Things, advanced addictive manufacturing, secure 5G and 6g telecommunication networks, as well as access to, and use of semiconductors. Domains where, leaving aside applications to defence, Europe shows clear gaps and delays if compared to the US and China. In particular, most recent developments focus on AI and data analytics as the source of competitive edge in warfare through 'data leadership', an area where Europe clearly lags behind. Re-Arm Europe rightly stresses the importance of the technological dimension and dual-use technologies, and the supporting White Paper[97] argues that competition in the new geopolitical context will revolve around such technologies, which are the main inputs for long-term economic growth and military pre-eminence. Because in such technologies the distinction between civilian and defence is blurred, evidently cutting-edge solutions that can improve military capabilities and operations may come from innovative civilian startups[98]. Investments in such disruptive technological innovations is fundamental to 'regain edge and prevent being technologically dependent'[99]. Dual-use technologies will play a key role, if the Re-Arm Europe ambitious goals of achieving European Defence Readiness by 2030 and build a 'European Defence Union' are to be met.

These goals appear very ambitious in view of the current state of play emerging from the analysis and considerations presented in Chapter 2. Europe has cumulated almost three decades of underinvestment in defence and started to increase expenditure and investments in sizeable fashion only after 2022. In particular investments in defence R&D and R&T have restarted after a long period of cuts and they are so far insufficient to keep pace with geopolitical rivals. The EU defence industry and market are fragmented both in terms of demand and supply. Both demand and supply are still mostly organised along national lines, with little European level collaboration, coordination, and integration, which highly limits the potential for the economy of scale needed. Not surprisingly, a very large amount of spending goes to third countries rather than remaining within the EU market. The fragmentation of demand is testified by the fact reported earlier that expenditure for equipment procurement in the EU is mostly spent on Commercial Off-The-Shelf (COTS) products procured from non-European manufacturers. It has been estimated, for instance, that between June 2022 and June 2023 out of a total of EUR 75 billion spent by Member States for equipment, 78% has been procured from outside the EU, out of which almost 63% from the US. There is a vicious circle between non harmonised demand and limited consolidation of EU suppliers. This circle further weakens the European Defence Technological and Industrial Base (EDTIB). If demand is not harmonised and aggregated, there is no possibility that the supply side is consolidated with the emergence of global level suppliers filling the capacity gaps. In dual-use technologies

and the defence tech sector emerging from them Europe lags five years behind the US. Moreover, Europe lags behind exactly in those civilian technologies that can have dual-use applications, and especially in AI. Europe, thus, needs to fill gaps and boost R&D in these areas. Finally, in the EU there has been traditionally, and there still is, a stronger separation between civilian and military research as compared to the US. The EU, with few exceptions (i.e., the Agence Innovation Defense is a small DARPA in France) has not had anything similar to DARPA and European universities and research centred have been so far reluctant toward the development of innovations to be applied in the defence industry. In reality, university-linked accelerators could be core actors in dual-use innovation. This is another source of fragmentation to be overcome if the EU has to develop both disruptive (mostly digital) technologies and their deployment in defence, creating an integrated bi-directional exchange between the two.

In the changing geopolitical context, in order to strengthen its defence industry and to modernise it through disruptive dual-use technological innovations, Europe face many challenges and sources of uncertainties. Among these, we consider that the most relevant ones are two: the level of European de-fragmentation of both demand and supply (or conversely persisting fragmentation) and the level and direction of private capital investment and public funding in dual-use technologies (including in R&D), which can create that level of business and market dynamism needed for the consolidation of supply and the emergence of many more global players than currently exist. As illustrated in the previous chapter, the EU defence industry is characterised by the presence of only a few large corporations with a global profile and by many SMEs remaining local players. Given the ambitious goal of Re-Arm Europe a key uncertainty is whether or not investments will be sufficient and effective to consolidate EU defence supply and facilitate the emergence of new global players of the scale of Airbus.

Overcoming the current fragmentation along national borders is crucial to reach economy of scale, rip efficiency gains, and avoid the costs of duplication. As stressed in the Letta Report, a Single EU Defence Market would enable the European defence industry to scale-up and grow[100]. The fragmentation of both demand and supply in the EU hampers the emergence of global suppliers and, at the same time, deprive innovative startups of the scale to market their innovations to large players across multiple national jurisdictions, limiting their ability to secure large defence contracts. Significant barriers remain in streamlining procurement and scaling dual-use innovations across Member States. Without more agile funding mechanisms and faster procurement processes, the EU defence actors may struggle to keep pace with global competitors. According to the Draghi Report[101], Europe lacks a strong focus on technological development and on R&D, especially for what concerns dual-use technologies that strongly require an EU-level scale rather than a national dimension. No single country can independently finance, develop, and sustain leadership in AI in defence, and other dual-use technologies. Therefore, the report proposed new dual-use programmes and European Defence Projects of Common Interest. Although Re-Arm Europe aims at achieving integration of efforts within an 'EU Defence Union' and put on the plate an envisioned 800 € billion investment, it remains unclear and uncertain to what extent these resources will follow established national level channels or will give rise to an EU integrated defence ecosystem that boosts defence in general and dual-use technologies in particular. So, one key uncertainty is whether in the future European fragmentation or de-fragmentation will prevail, which to a large extent depends on the actions that the 'shapers' will undertake in terms of regulation and policies aimed at supporting de-fragmentation.

The other key uncertainty concerns the 'makers' and is about the extent to which private capital and public funding for dual-use technologies will trigger business and market dynamism leading to supply consolidation. Mobilising private capital is among the five mechanisms for a surge in defence spending envisioned in the above cited 2025 White Paper[102]. As we next show, public funding has an important role to play and can catalyse development but is

insufficient. Private capital inflows are particularly important for the EU to fill the gap vis-à-vis the US in dual-use technologies. Increased defence spending, technological advancements and the dual-use nature of technologies are driving private investors' interest in the defence and dual-use technology sector. On the other hand, challenges related to defence procurement and the need for caution in military technology investments remain relevant considerations for investors, even when considering dual-use technologies. Barriers still exist that limit investments: complexity and length of procurement procedure in the defence sector limiting visibility of market potential; sector-specific regulations introducing complexities and higher costs. Barriers derive also from a too strict interpretation of the Environmental, Social and Governance (ESG), which leads banks and investment funds in the EU not to invest in the dual-use technologies with application to the defence sector. Not surprisingly, among the priorities of the Commission in 2025 is that of presenting a Defence Omnibus Simplification proposal[103] that will concern, among others, regulatory simplification and harmonisation on rules and procedures for defence procurement[104], and 'removing obstacles related to access to finance, including Environmental, Social and Governance investment'[105]. Support from dedicated public funding is also fundamental to bridge the gaps and boost investments in dual-use R&D. In this respect, besides the amount of funding, it is also important how they are provided given the specific nature of dual-use technologies. As illustrated in paragraph 2.3.2, historically the EU has kept R&D funding for civilian and military innovation separated, which resulted in parallel ecosystems with distinct stakeholder communities, objectives, regulatory frameworks, and funding instruments. Recent developments suggest a move from separation to convergence. There is a growing orientation to integrate funding mechanisms, since investment in dual-use technologies could enhance both the EU's competitiveness and its defence capabilities. Yet, it is yet to be seen if in the future such orientation will materialise, with two possibilities being represented: a) dual-use research funded under the new FP10; and/or b) establishment, as a stand-alone funding instrument, of a new Dual-Use Fund. Or, rather, only gradual changes will be introduced.

THE PROPOSED SCENARIOS

So, given the main uncertainties described above, for the definition of the four scenarios visually presented in the picture below, the two axes chosen concern, as in the tradition of these reports series, both the 'shapers' (horizontal axe) and the 'makers' (vertical axe). The 'shapers' axe is about the extent to which regulatory and policy efforts have a defragmentation effect leading to the harmonisation of demand (varying from strong to weak). The 'makers' axe is the extent to which private capital and public funding trigger business and market dynamism and give rise to a more consolidated supply (also varying from strong to weak).

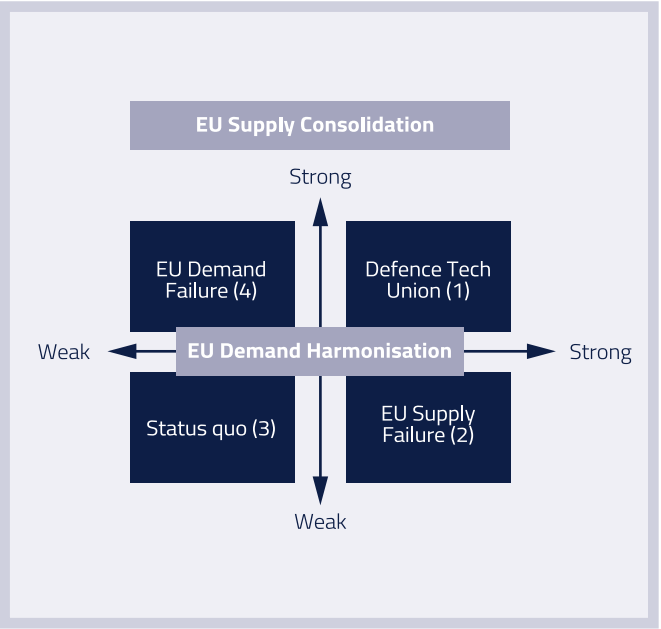

Figure 6 Proposed scenarios, Source: Authors' elaboration

SCENARIOS' STORYLINES

Defence Tech Union (Scenario 1).
The vision behind this scenario is that the EU becomes a global leader in dual-use innovation through a tightly coordinated public-private ecosystem. The main strategic outcome is that the EU achieves strategic autonomy and technological sovereignty, and becomes a trusted exporter of secure, ethical dual-use technologies. This occurs because at the same time demand is harmonised and supply consolidated. As a result of the emergence of an EU Defence Tech Union and of a unified defence single market, increased scale and collaboration also enables the strengthening of an EU Tech ecosystem, with catching up in AI, semiconductors, and other digital technologies. The new EU ecosystem becomes one where both EU defence and EU digital technologies thrive in dual-use applications, with decreased need of digital technologies imported from outside the EU. EU institutions and member states act decisively to integrate funding, procurement, and regulation. Public policy mobilises and de-risks massive private investments. A thriving dual-use tech ecosystem emerges across Europe with a balance of civil-military innovation. This scenario sees the EU successfully aligning policy, regulation, and funding to stimulate a vibrant dual-use tech ecosystem. Strong public-private cooperation, shared standards, and cross-border collaboration drive scale and strategic autonomy. Examples of such new level of integration include: a) the establishment of a Pan-European and fully operational 'EU Dual-Use Tech Fund' functioning both as direct funding and as fund of funds; b) the set-up of a Defense Innovation Council and of a joint procurement mechanism under EU umbrella; c) EU-wide joint programs on drone defence system and secure telecommunications 5g and 6G platform embedding AI and data analytics co-developed with NATO partners; and d) creation of a EU level DARPA-like agency activng as first buyer of emerging technologies. This scenario presents a number of key features. First, the emergence of EU-wide procurement and standards increase economy of scale for suppliers and increases inter-operability for dual-use defence technologies. Second, public funding to dual use technologies is provided in integrated fashion to civilian and defence applications, while the reduction of risks and complexities through the creation of stable regulatory environments stimulate robust private investment in dual-use technologies. Third, as a result of both regulatory streamlining and strong investments, an accelerated tech maturation in areas like AI, cybersecurity, space, and quantum with civil and defence applications takes place. Fourth, public-private partnerships bridge industry and defence taking innovation from the labs to deployment. Among the positive effects of this scenario the following are worth mentioning. Europe can achieve global leadership in the production and market diffusion of responsible and ethical dual-use applications. It increases the potential for export and strategic partnership with allies with Europe in the driving sit and capable of defining what capacities dual-use technologies should have when used in defence applications. Europe can achieve resilience in critical sectors such as semiconductors and communications. Innovation is high and has positive spill-over effects on economic growth and competitiveness of industry. A balanced civil-military tech pipeline supports European security and industrial competitiveness. On the other hand, the strong regulatory and policy integration run the risk of over-centralisation and bureaucratic delays, while the new assertiveness of Europe and its increased technological sovereignty may give rise to geopolitical tensions.

EU Supply Failure (Scenario 2).
The vision behind this scenario is that dual-use innovation is driven by public institutions, but market engagement lags. Policy and regulation enable the harmonisation of EU demand, but consolidation of the supply side fails to emerge. The main strategic outcome is that the EU becomes a capable but inward-looking innovator, struggling to scale solutions or attract market momentum. EU builds strong governance and funding structures (e.g. Dual-Use Fund, simplified procurement), but business interest remains low. Innovation is policy-driven, and uptake is uneven; the EU struggles to commercialise and scale innovations. The EU sets up ambitious governance and funding mechanisms

but fails to attract robust business engagement. Examples of such situation include, for instance: a) a centralised EU AI-for-defence research program generate only few spinouts or startups and b) underutilized innovation capacity due to lack of incentives for private developers; Innovation is primarily driven by public actors, with limited private sector uptake or commercial viability. Innovation remains state-led and policy-dependent, with few scalable ventures, which causes the gap between research and commercialization persists. In the absence of a robust inflow of private capital, the development of dual-use technologies heavily relies on state-driven R&D and public procurement. This limits the bridging from the labs to deployment. As a result, innovation hubs remain policy-dependent and less competitive at global level because of limited scalability of dual-use innovations in the absence of a strong market pull. There is, on the other hand, the potential of seedbed foundational R&D leading to mission-driven innovation. This potential, however, can only materialise if success stories emerge that can attract capital investments and market players, thus, achieving both security objectives and increased competitiveness. In this scenario, heavily reliant on public top-down push and public funding of R&D, the main risk is related to the so-called 'valley of death' between the lab and the market, which hampers the tech maturation in areas like AI, cybersecurity, space, and quantum with civil and defence applications and can lead to a misalignment between military and civilian tech needs. The limited scalability of European dual-use technologies at global level prevents the EU from establishing principles and standards for responsible and ethical application in the defence domain.

Status quo (Scenario 3).
The vision behind this scenario is that the EU fails to coordinate and/or invest effectively in dual-use innovation. The main strategic outcome is that the EU loses ground in both civil and defence tech, eroding its strategic autonomy, technological sovereignty and resilience. Neither business nor policy actors manage to step up. The EU remains fragmented, underinvested, and slow. Dual-use innovation is weak, and Europe loses ground to global rivals. Europe fails to mobilize either public policy or market dynamism. Fragmentation, underinvestment, and strategic inertia lead to stagnation in dual-use innovation. Dependency on non-EU technology deepens, undermining autonomy. Examples of such situation include, for instance: a) reliance on third-country suppliers (mostly US) for key security technologies; b) brain drain and startup exodus to Silicon Valley or Asia. The EU and Member States fails to build a coherent governance with a common vision for the Defence Industry and dual-use technologies. Procurement and demand remain fragmented and disjointed, regulatory complexities and uncertainties remain, which disincentivise private capital investment and business dynamism. Furthermore, no EU-wide public funding mechanism for dual-use technologies is introduced. The failed aggregation (de-fragmentation) of demand cause the persistent fragmentation of supply and production given that scale is not achieved and markets continue to function mostly along national borders and practices. As a result, rather than by an accelerated tech maturation in areas like AI, cybersecurity, space, and quantum with civil and defence applications, this scenario is characterised by a deceleration in these technological areas with divergence between civilian and defence technology, which cause increased delays and gaps of the EU vis-à-vis it main geopolitical competitors. With stagnant innovation and with almost absent bridging from the labs to deployment, talent and capital flow to more dynamic regional ecosystems (i.e., US and Asia). Dependency on non-EU tech and defence solutions deepens. No compelling policy or market forces mobilize the ecosystem. Europe becomes increasingly dependent on external technologies and suppliers. Innovation is fragmented, slow, and fails to meet emerging security challenges. Under such conditions the EU runs the risks of seeing an erosion of its industrial competitiveness and security readiness, which can undermine its geopolitical relevance by deepening technological (mostly digital technologies) and defence dependency. With stagnant innovation there is no effect on economic growth. Finally, what responsible and ethical use of dual-use technologies in defence applications means is entirely determined by its global geopolitical competitors, while the EU is entirely left out.

EU Demand Failure (Scenario 4).
The vision behind this scenario is that the national or regional champions drive innovation and produce some level of supply consolidation without, however, an EU-level coherent harmonisation of demand. The lack of a harmonised EU demand limits the potential of supply consolidation, with new global players forced to reach markets outside the EU. The main strategic outcome is that the EU has innovative clusters but without achieving strategic coherence and integration, which limits its influence and global competitiveness. Innovative businesses and investors drive progress, but in silos across different national markets. Fragmented regulation and lack of coordination limit scale, cross-border R&D, and interoperability. EU strategic autonomy and technological sovereignty remains limited. Because Lack of regulatory alignment and joint procurement hinders cross-border collaboration, private-sector players thrive in disconnected national ecosystems. Startups, scale-ups, and national champions flourish in isolated national ecosystems. Despite vibrant innovation in some regions, lack of EU coordination hampers interoperability, scaling, and strategic cohesion. As a result, EU-wide strategic goals are undermined by fragmentation and competition between Member States. Innovation is driven by venture capital and national interests, and not by EU policy, which causes misalignment between military and civilian tech needs. Because the regulatory and procurement landscape have not been defragmented, duplication and inefficiency characterise the EU defence and dual-use technology ecosystem. So, regional hubs emerge, but with limited cross-border integration. Examples of such situation include, for instance: a) national drone, AI, or satellite programs that compete rather than integrate; b) disjointed export controls and security protocols across member states. An accelerated tech maturation in areas like AI, cybersecurity, space, and quantum with civil and defence applications takes place in a scattered fashion, so that there are a few advanced regional clusters but this is not evenly spread in the EU that is, thus, characterised by the presence of main internal regions that lags behind in dual-use technologies defence applications. This scenario is characterised by the presence of opportunities for agile and fast-moving innovation in high-tech sectors. These remain, however, expressions of national or even regional level leadership in niche domains, with no EU-level scalability across all relevant technological domains. This scenario is characterised by two major risks. First, that lack of strategic coherence and integration at EU-level can give raise to some forms of technological nationalism. Second, that the lack of EU-wide alignment can create vulnerability to external dependencies, at least for some technologies and in large parts of the EU. Because the bridging from the lab to deployment remains fragmented and limited to niche domains, equally fragmented and limited are the effects in term of industrial competitiveness, economic growth, and security resilience.

SCENARIOS ASSESSMENT AND CONCLUSIONS

The picture below provides a qualitative assessment of the four scenarios along six dimensions. Going clock-wise the first is abbreviated as 'Growth', referring to economic growth impacts of the scenarios. Innovation and competitiveness are in a sense subsumed under this dimension as they can be considered as intermediate outcome that shape the economic growth impact. Second, there is the effect on strengthening the European Defence Technological and Industrial Base (EDTIB). Third, scenarios are assessed to the extent they promote strategic autonomy of the EU, which for the sake of simplicity is assumed to include as a key component also technological sovereignty. Fourth, there is the dimension of whether the scenarios contribute to create high-tech jobs as a result of innovation (or lack thereof) in dual use technologies. The fifth dimension summarised as 'EU Security' refers to the level of security readiness of the EU Defence, including supply chain resilience. Finally, 'EU Responsible Leadership' refers to the capacity of imposing standards for a transparent and ethical governance of dual-use technologies in defence applications, which in turn would contribute to build support to, and trust in, EU institutions in the citizenry.

As intuitively visible from the above diagram, Scenario 1 (Defence Tech Union) is dominant and superior on all six dimensions compared to the other three scenarios. The harmonisation of demand and the consolidation of supply, as well as the increased EU-level scale foster dual-use technologies innovation and industrial competitiveness with clear and sizeable spillover on economic growth. This in turn strengthen the European Defence Technological and Industrial Base (EDTIB), which brings also a fairly high level of technological sovereignty and strategic autonomy as the EU become a global level player in dual-use defence technologies. Although strategic autonomy cannot reach the maximum score, since even under this scenario some level of external dependency remain. The accelerated tech maturation in areas like AI, cybersecurity, space, and quantum with civil and defence applications feed the labour market and opens opportunities for the creation of high-tech jobs. The increased cross-border dimension and the strengthening of the industrial base ensures EU defence readiness and resilience. Finally, because the EU is in the driving sit and can steer what is a responsible and ethical use of dual-use technologies in defence applications, this means responsible leadership is exerted, producing social support and acceptance and increased trust in EU institutions that increase their legitimacy.

On the opposite extreme of the spectrum, Scenario 3 (Status quo) is clearly the one with the least positive impacts. In this scenario we have stagnation in high-tech sectors, reliance on non-EU suppliers and loss of competitiveness in key areas like AI, space, or defence. So, decreased innovation leads to lower productivity and economic growth. The persistent fragmentation of demand and little consolidation of supply with limited market scale prevent the strengthening of the European Defence Technological and Industrial Base (EDTIB). Growing dependency weaken technological sovereignty and strategic autonomy. Stagnant innovation in dual-use technology prevent the creation of high-tech jobs and rather causes brain drain as talent and startups migrate to the U.S. or Asia. The almost inexistent cross-border dimension and the related weakening of the industrial base greatly reduce EU defence readiness and resilience, which contributes to rising

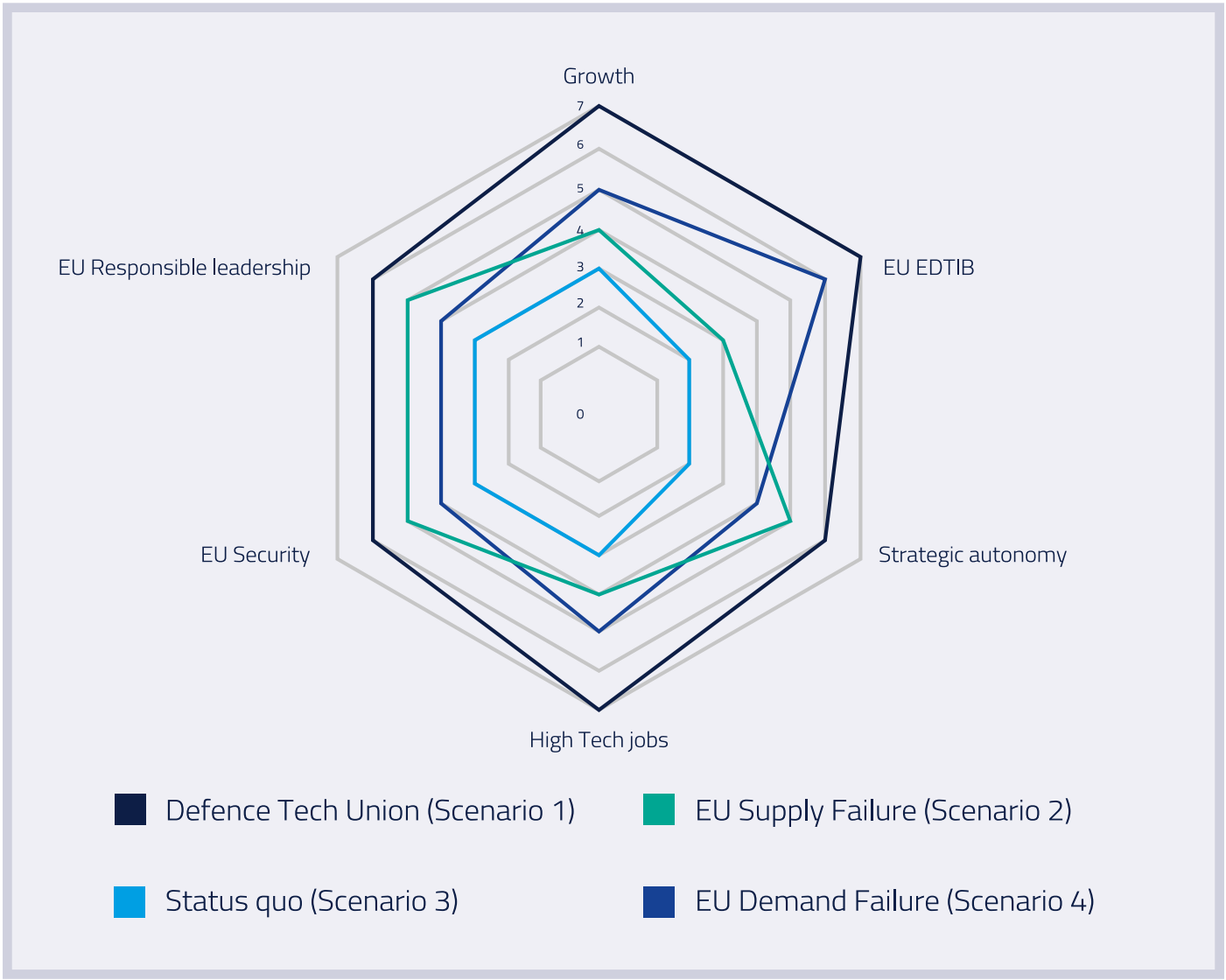

Figure 7 Radar diagram scenarios assessment, Source: Authors' elaboration

geopolitical anxiety and public demand for stronger sovereignty. This in turn decreases support to, and trust in, the effectiveness of EU institutions that are not in the condition of exerting responsible leadership, and weakens democratic resilience as Europe relies on foreign-controlled digital infrastructure.

The other two intermediate scenarios show mixed impacts and can be placed in between the two extreme scenarios. Here, we briefly compare one with the other. In Scenario 2 (EU Supply Failure) the harmonisation of demand gives at least the EU buying power and a limited possibility to impose some standards, which means scores in strategic autonomy, EU Security, and EU responsible leadership higher compared to the other intermediate scenario (Scenario 4, EU Demand Failure). On the other hand, because of the presence of some consolidation in supply, Scenario 4 is higher on growth and on the industrial base, and on the creation of tech jobs but obviously lower than Scenario 1. While because of lack of harmonisation there is not an internal demand, under Scenario 4 we can envisage a few EU consolidated players becoming global suppliers, which is why the scenario score relatively higher on growth and industrial base.

In view of the description and assessment of the scenarios the following strategic implications and recommendations can be drawn:

1. The "Defence Tech Union" is clearly the most desirable path potentially delivering many positive impacts. To move toward this ideal scenario shapers and makers must join forces and implement bold and synchronized actions supporting the harmonisation of demand and the consolidation of supply. Such actions would help avoid drifting in the status quo as weak policy or market inertia might lead to an irreversible decline in Europe's strategic geopolitical position.
2. The main policy levers include Investment in EU-wide standards, collaborative cross-border procurement, and regulatory simplification, as the main triggers to catalyse capital investors and business interest.
3. There is a need for stronger alignment in strategic areas like chips, battery technology, semiconductors, and AI and that defence and technology advancements go hand in hand. Currently, in the EU we have the Re-Arm Europe package with € 800 billions of investment involving defence ministries and the AI package with € 200 billions of investment involving innovation ministries. These two packages should be aligned and integrated if EU dual-use technologies are to benefit both defence readiness and economy and society resilience.
4. Incentivising scale-ups, private R&D, and dual-use startups is essential for ecosystem vitality. Dual-use means developing two strong pillars hand in hand and requires tearing down the traditional separation between civilian and military innovation, including through the establishment of integrated public funding of R&D in dual-use technologies.
5. If the EU is to control the conditions for responsible and ethical dual-use technologies in defence applications, it needs a strong position in both field. The EU should think about the principles about how to use dual-use, such as through a Dual-Use Act, establishing the rules for the application of new technologies in warfare.

ACKNOWLEDGEMENTS

This report on "Digital and Defence Innovation for Europe's Strategic Autonomy" is part of the 28DIGITAL Makers & Shapers report series. These reports address specific aspects of digital technologies and developments. They follow a scenario-based approach, grounded in the state of the art in the specific field, and analyse the impact of different scenarios on predefined indicators.

Cristiano Codagnone was contracted to support the study and write this report under the guidance and supervision of 28DIGITAL. We acknowledge their contribution, assisted by Giovanni Liva, for providing breadth and depth to the study via interdisciplinary stakeholder discussions, as well as extensive literature analysis and survey.

We would also like to thank the following experts for reviewing the report and providing invaluable input to this study:

Alexandru Sarbu, Investment Manager, TechCelerator, Andris Baumanis, Chairman, Unilab – leading the establishment of NATO DIANA Accelerator in Riga, Antonella Di Trapani, Executive in Residence Fellow, Geneva Centre for Security Policy, Bence Hovarth, Cyber Defence Director, Benjamin Schulte, Strategy & Innovation Lead, Capgemini, Bodgan Popovici, Consultant, Romanian Tech Startups Association (ROTSA), Cedric Lowenbach, Defense Representative – Development Director, Bpifrance, Christian van der Woude, Ecosystem Interventions & Government Affairs Lead, TechLeap.NL, Claudia Gherman, Digital Transformation Senior Manager, ASD Europe, Cristian Dascalu, Managing Partner & Co-founder, TechCelerator, Eoin O'Connell, Associate Professor, Department of Electronics & Computer Engineering, University of Limerick, Felikss Bikaunieks, Senior Expert, Entrepreneurship Competitiveness Department, Ministry of Economics of the Republic of Latvia, Florian Schlüter, Chief Digital Officer, Renk Group, Fran Ferrera, Brussels Representative for Institutional and Industrial Relations in Defence, Security, Space, and Sovereign Digital Technologies, SopraSteria, Francesco Bonfiglio, CEO & Co-founder, Dynamo – The European Cloud Alternative, Gabriel Jory, Defence & Security Manager, ASD Europe, Gerasimos Michalitsis, Chief Technology Officer, Netcompany SEE & EUI, Giuseppe Lacerenza, Partner, Keen Venture Partners, Henri Schasmin, Coordinator for Protection of Personal Data and State Secrets, Defence and Security Coordinator, TalTech, Ilze Lore, Director of Entrepreneurship Support Department, Ministry of Economics of the Republic of Latvia, Janis Kondrats, Project Manager – EDF Programme Coordinator, Riga Technical University Science and Innovation Centre, Javier Lopez, Professor of Computer Science, University of Malaga, Jesus Angel García, Head of R&D and Universities, Indra, Klaus Beetz, Former CEO, EIT Manufacturing, Kristina Boseva, Investment Manager, IMPETUS Capital, Laure Blanchard-Brunac, Member of the Research, Innovation and Digitisation Window (RIDW), InvestEU Investment Committee, Liam Crane, CTO, Nokia Space and Defense, Linnar Viik, Archangel Ventures, Lukas Roffel, Chief Technical Officer, Thales Nederland, Maarten Cleeren, Managing Director, TechLeap.NL, Mihkel Tedremaa, Product Development Manager, Seventh Sense OÜ, Nikolaos Loutas, Director Innovation, NATO, Olivier Blazy, Vice-president of the Department of Computer Science, Institut Polytechnique de Paris, Oleksandr Bulatnikov, DeepTech VC Investor, Presto Ventures, Panagiotis Papageorgiou, Executive Board Member, Hellenic Center for Defence Innovation, Raivis Supe, Ministry of Economics of the Republic of Latvia, Selmar Smit, Science & Technology Manager Autonomous Systems & Decision Support, TNO, Stefan Op de Beek, Cybersecurity Expert, TU Delft, Sven Weizenegger, Head, Cyber Innovation Hub, Bundeswehr (Germany), Tõnis Segerkrantz, Head of Innovation, AI & Robotics Estonia (AIRE), Umit Cayan, Global Government Affairs & Business Development Lead for Defence, SAP.

REFERENCES

1. Ursula von der Leyen, Candidate for the European Commission President, Political Guidelines for the Next European Commission, 2024-2029, Strasbourg 18 July 2024 (https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb-2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf).
2. https://ec.europa.eu/commission/presscorner/detail/sv/statement_25_673.
3. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 19 March 2025 White Paper: For European Defence Readiness 2030 (JOIN(2025) 120 final) (https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf).
4. Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021, setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0821.
5. European Commission, (2025). Foresight Report 2025. Resilience 2.0: Empowering the EU to Thrive Amid Turbulence and Uncertainty, Luxembourgh, Publication Office of the European Union (https://commission.europa.eu/document/download/bdba60f0-abb3-42f8-b5be-fd35d693b289_en?filename=SFR2025-Report_web.pdf).
6. European Commission, Proposal for a Regulation of the European Parliament on establishing the European Competitiveness Fund ('ECF'), including the specific programme for defence research and innovation activities, repealing Regulations (EU) 2021/522, (EU) 2021/694, (EU) 2021/697, (EU) 2021/783, repealing provisions of Regulations (EU) 2021/696, (EU) 2023/588, and amending Regulation (EU) [EDIP], Brussels 16.7.2025, COM(2025) 555 final (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2025:555:FIN), p. 21.
7. Keynote speech by President von der Leyen at the European Defence Agency (EDA)Annual Conference 2023: Powering up European Defence, 30.11.2023 (https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_23_6207)
8. Baldwin, H. Critical dual-use technologies: commercial, regulatory, societal and national security challenges. NATO General Report, 26 August 2024 (https://www.nato-pa.int/download-file?filename=/sites/default/files/2024-12/051%20ESC%2024%20E%20rev.2%20fin%20-%20CRITICAL%20DUAL-USE%20TECHNOLOGIES%20-%20BALDWIN%20REPORT.pdf).
9. Christian Haddad, Dagmar Vorlíček & Nina Klimburg-Witjes (2024) The Security-Innovation Nexus in (Geo-)Political Imagination, Geopolitics, 29:3, 741-764, DOI: 10.1080/14650045.2024.2329940, p. 748.
10. Raluca Csernatoni & Bruno Oliveira Martins (2024) Disruptive Technologies for Security and Defence, op. cit.
11. Thomas McSorley, Maciel Macenowicz, Matthew Maddison, & Christopher R. Yukins (2025)., Allies Bridging The Valley Of Death: How NATO's Defence Innovation Accelerator For The North Atlantic Will Help Maintain NATO's Technological Edge (January 08, 2025). GWU Legal Studies Research Paper 2025-04, GWU Law School Public Law Research Paper 2025-04 (https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=3029&context=faculty_publications). See also: https://www.nato.int/cps/en/natohq/official_texts_236539.htm; and https://www.digitaleurope.org/resources/redefining-defence-innovation-an-industry-blueprint-for-natos-rapid-adoption-action-plan/.
12. See: https://eda.europa.eu/news-and-events/news/2022/05/17/hub-for-eu-defence-innovation-established-within-eda.
13. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 19 March 2025 White Paper: For European Defence Readiness 2030, op. cit., p. 3.

14. Clapp, S. EU Member States' defence budgets, EPRS | European Parliamentary Research Service, 772.846 – May 2025 (https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/772846/EPRS_ATA(2025)772846_EN.pdf).
15. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 19 March 2025 White Paper: For European Defence Readiness 2030, op. cit., p. 4.
16. Soler, P. 'How can the EU unlock up to €800bn for its 'rearmament plan'? Euronews, 5 March 2025 (https://www.euronews.com/my-europe/2025/03/05/how-can-the-eu-unlock-up-to-800bn-for-its-rearmament-plan?utm_source=news.google.com&utm_campaign=feeds_bcs_topstories&utm_medium=referral).
17. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 19 March 2025 White Paper: For European Defence Readiness 2030, op. cit., p. 4.
18. Ibid., p. 15.
19. The database is updated annually and can be downloaded at: https://www.sipri.org/sites/default/files/SIPRI-Milex-data-1948-2023_0.xlsx. SIPRI also publishes yearly a Yearbook on Armaments, Disarmament and International Security.
20. See the gap analysis in : a) Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 18 May 2022 on the Defence Investment Gaps Analysis and Way Forward (JOIN(2022)0024) (https://www.europarl.europa.eu/doceo/document/TA-10-2025-0034_EN.pdf); and Clapp, S. Reinforcing European Defence Industry, EPRS | European Parliamentary Research Service, PE 749.805 – November 2024 (https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/749805/EPRS_BRI(2023)749805_EN.pdf).
21. The Draghi report: A competitiveness strategy for Europe, 9 September, 2024 (https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?filename=The%20future%20of%20European%20competitiveness%20_%20A%20competitiveness%20strategy%20for%20Europe.pdf).
22. Niinistö, S. Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness, 30 October 2024 (https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf).
23. Commission Staff Working Document, for a European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products, of 8 July 2024 (C(2024) 4822 final) (https://defence-industry-space.ec.europa.eu/document/download/f1e6ba44-4720-4f14-a991-a3a7f3afb475_en?filename=Staff%20Working%20Document%20on%20EDIP.PDF), p. 10.
24. EDA, 'Defence data 2023-2024', Brussels 2024 (https://eda.europa.eu/docs/default-source/brochures/1eda---defence-data-23-24---web---v3.pdf).
25. We have compared 2023 with 2021, as this was the latest year where data on European Collaborative Defence Equipment Procurement Expenditure and Collaborative Defence R&T Expenditure were available, which are important to characterise the level of integration. Such data are not yet available for 2022 and 2023.
26. EDA, 'Coordinated Annual Review on Defence: Report 2024', Brussels 2024 (https://eda.europa.eu/docs/default-source/documents/card-report-2024.pdf), p.
27. EDA, 'Defence data 2023-2024', op. cit., p. 9.
28. Maulny, J-P., 'The Impact of the War in Ukraine on the European Defence Market', IRIS Policy Paper, 2023 (https://www.iris-france.org/wp-content/uploads/2023/09/19_ProgEuropeIndusDef_JP-Maulny.pdf).
29. EDA, 'Defence data 2023-2024', op. cit., p. 9.
30. Office of the Under Secretary of Defense (Comptroller) (2023): National Defense Budget Estimates for FY 2024, available at: National Defense Budget Estimates for FY 2024 (https://comptroller.defense.gov/portals/45/documents/defbudget/fy2024/fy24_green_book.pdf). The US definition of RDT&E and EDA's definition of R&D are broadly comparable.
31. SIPRI Factsheet: Trends in World Military Expenditure, 2023 (https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf).

32. SIPRI 2023 yearbook database (https://www.sipri.org/yearbook/2023).
33. See for instance Clapp, S. Reinforcing European Defence Industry, op. cit. The persisting gaps are also stressed in the earlier cited 2025 White Paper (Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 19 March 2025 White Paper: For European Defence Readiness 2030, op. cit), the 2022 Joint communication (Joint Communication of May 22: Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 18 May 2022 on the Defence Investment Gaps Analysis and Way Forward, op. cit.), and in the 2024 SWD (Commission Staff Working Document, for a European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products, op. cit.).
34. Commission Staff Working Document, for a European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products, op. cit., p. 14.
35. Ibid.
36. Clapp, S. Reinforcing European Defence Industry, op. cit., p. 3.
37. EDA, 'Defence data 2022', Brussels 2023 (https://eda.europa.eu/docs/default-source/brochures/2022-eda_defencedata_web.pdf).
38. EDA, 'Coordinated Annual Review on Defence: Report 2022', Brussels 2022 (https://eda.europa.eu/docs/default-source/eda-publications/2022-card-report.pdf), p. 7.
39. https://www.reuters.com/markets/europe/france-raise-5-bln-euros-defence-sector-funding-finance-minister-says-2025-03-20/
40. https://www.cyberinnovationhub.de/en/about-us
41. See: https://securitydelta.nl/news/overview/launch-defport-towards-acceleration-innovation-faster-production-of-military-equipment.
42. See: https://www.secfund.nl/en.
43. See: https://www.mod.gov.lv/lv/dronu-koalicija-0.
44. EDA, 'Defence data 2023-2024', op. cit., p. 11.
45. See: https://eudis.europa.eu/index_en.
46. See: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=R%26D_expenditure
47. Office of the Under Secretary of Defense (Comptroller) (2023): National Defense Budget Estimates for FY 2024, available at: National Defense Budget Estimates for FY 2024 (https://comptroller.defense.gov/portals/45/documents/defbudget/fy2024/fy24_green_book.pdf). The US definition of RDT&E and EDA's definition of R&D are broadly comparable.
48. SIPRI 2023 yearbook database (https://www.sipri.org/yearbook/2023).
49. European Commission, Access to equity financing for European defence SMEs, Publications Office of the European Union, 2024 (https://data.europa.eu/doi/10.2889/698738).
50. Boroush, M. (2020). Research and Development: US Trends and International Comparisons. Science and Engineering Indicators 2020. NSB-2020-3. National Science Foundation.
51. https://ncses.nsf.gov/pubs/nsb20246/executive-summary
52. Gargalakos, M. (2024). The role of unmanned aerial vehicles in military communications: application scenarios, current trends, and beyond. The Journal of Defense Modeling and Simulation, 21(3), 313-321.
53. https://www.newyorker.com/magazine/2022/05/16/the-turkish-drone-that-changed-the-nature-of-warfare
54. See, for instance, the coverage of this operation by The Guardian: https://www.theguardian.com/world/2025/jun/02/operation-spiderweb-visual-guide-ukraine-drone-attack-russian-aircraft.
55. https://interpret.csis.org/translations/starlink-militarization-challenges-and-responses-to-space-intelligence-and-information-security/
56. https://www.darpa.mil/research/programs/blackjack
57. https://defensetalks.com/united-states-project-maven-and-the-rise-of-ai-assisted-warfare/
58. See a review of such applications in Miličević, Z. & Bojković, Z. (2024). Review of 5G and 6G applications for mobile wireless communication in the military environment, Vojnotehnički Glasnik / Military Technical Courier, 72 (1), pp. 435-451 (https://scindeks-clanci.ceon.rs/data/pdf/0042-8469/2024/0042-84692401435M.pdf).
59. See: Dzogovic, B. & Holtmanns, S. (2024). Securing 5G Communication in Joint Operations Between NATO Partners, in Kwan, C. et al. (eds), CyCon 2024: Over the Horizon 16th International Conference on Cyber Conflict, pp. 29-46. Tallin: NATO CCDCOE Publications

(https://ccdcoe.org/uploads/2024/05/CyCon_2024_Dzogovic_Holtmanns-1.pdf).
60. Thornhill, J. 'The Appetite for U.S. Defence Tech Is Growing' , Financial Times, 19 August 2024 (https://www.ft.com/content/9b9e-13de-f708-4c68-9a0d-4a4e9243a83e?utm_source=chatgpt.com).
61. Metinko, C. 'Defense Tech Venture Funding Gains Traction', Crunchbase News, 12 February 2025 (https://news.crunchbase.com/venture/defense-tech-funding-growth-yir-2024/).
62. Klempner, J., Rodriguez, C., & Swartz, D. (2024). A rising wave of tech disruptors: The future of defense innovation?. McKinsey and Company. (https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/a-rising-wave-of-tech-disruptors-the-future-of-defense-innovation).
63. https://www.wsj.com/tech/ai/openai-enters-silicon-valleys-hot-new-business-war-7beccf6e?utm_source=chatgpt.com.
64. https://dealroom.co/uploaded/2025/02/NIF-report-Defence-Security-and-Resilience-2025-1739358861.pdf?x63517
65. https://dealroom.co/uploaded/2024/07/Dealroom-Europe-Q2-2024-VC-Report.pdf?x90202
66. https://warontherocks.com/2022/09/reliance-on-dual-use-technology-is-a-trap/
67. Edler, J., Blind, K., Kroll, H., Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. Research Policy, 52, 104765.
68. Trippl, M., Soete, L., Kivimaa, P., Serger, S. S., Koundouri, P., & Pontikakis, D. (2024). Addressing the regional dimension of open strategic autonomy and European green industrial policy. Publications Office of the European Union.
69. Soete, L., & Burgelman, J. C. (2023). Reconciling Open Science with Technological Sovereignty: Can the European Union do it?. J. Open Access L., 11, 1.
70. Crespi F., Caravella S., Menghini M. and Salvatori C. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy. Intereconomics, 6, 348-354.
71. OECD Science, Technology and Innovation Outlook 2023. Enabling Transitions in Times of Disruption. Paris: OECD.
72. https://www.wassenaar.org/
73. NATO (2024). Critical dual-use technologies: commercial, regulatory, societal and national security challenges. General Report. Economics and Security Committee.
74. https://www.bis.gov/press-release/commerce-strengthens-export-controls-restrict-chinas-capability-produce-advanced
75. Informal meeting of the Heads of State or Government, Versailles Declaration, 11 March 2022 (https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf).
76. Council of the European Union 7371/22.
77. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 20 June 2023, On European Economic Security Strategy (JOIN (2023) 20 final) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020).
78. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 5 March 2024 on A new European Defence Industrial Strategy: Achieving EU readiness through a responsive and resilient European Defence Industry (JOIN(2024)10 final) (https://defence-industry-space.ec.europa.eu/document/download/643c4a00-0da9-4768-83cd-a5628f5c3063_en?filename=EDIS%20Joint%20Communication.pdf).
79. Proposal for a regulation of the European Parliament and of the Council establishing the European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products ('EDIP'), 5 March 2024 (COM (2024) 150 Final) (https://defence-industry-space.ec.europa.eu/document/download/6cd3b158-d11a-4ac4-8298-91491e5fa424_en?filename=EDIP%20Proposal%20for%20a%20Regulation.pdf).
80. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 19 March 2025 White Paper: For European Defence Readiness 2030, op. cit. In the following paragraphs we summarise the key aspects of this White Paper.
81. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 19 March 2025 White Paper: For European Defence Readiness 2030, op. cit., p. 4.

82. Ibid., p. 15.
83. Ibid., p. 15.
84. Ibid., p. 15.
85. It must be noted, however, that about the new EIB approach and mandate so far there have been a lot of communication but no final firm text has been adopted. So, the new role of the EIB at the moment remains a possibility rather than a certainty.
86. Burton, S. D., Aicardi, C., Mahfoud, T., & Rose, N. (2018). Understanding interstate competitiveness and international security in European dual-use research. In Biomimetic and Biohybrid Systems: 7th International Conference, Living Machines 2018, Paris, France, July 17–20, 2018, Proceedings 7 (pp. 129-133). Springer International Publishing.
87. European Commission, A competitive Europe for a sustainable future, Publications Office of the European Union, 2024, https://data.europa.eu/doi/10.2777/965670
88. European Commission, Communication On options for enhancing support for research and development involving technologies with dual-use potential, Brussels, 24.1.2024, COM(2024) 27 final (https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_white-paper-dual-use-potential.pdf).
89. Schwaag Serger, S. et al. (2023). Research, innovation, and technology policy in times of geopolitical competition, August, ESIR paper.
90. Examples include the: a) European Commission, Communication on Action plan on synergies between civil, defence and space industries, Brussels, 22.02.2021COM(2021) 70 final 2021(https://commission.europa.eu/document/download/2353ded9-0e39-4d35-a46c-67c62779afe1_en?filename=action_plan_on_synergies_en.pdf); b) European Commission, Communication on Roadmap on critical technologies for security and defence, Strasbourg, 15.2.2022, COM(2022) 61 final(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0061); and c) the Joint Communication, Defence investment gaps analysis and way forward, op.cit.
91. European Commission, White Paper on On options for enhancing support for research and development involving technologies with dual-use potential, Brussels, 24.1.2024, COM(2024) 27 final (https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_white-paper-dual-use-potential.pdf).
92. The Draghi report: A competitiveness strategy for Europe, op. cit.
93. European Commission, Communication on The EU Startup and Scaleup Strategy. Choose Europe to start and scale, Brussels 28.5.2025, COM(2025) 270 final (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52025DC0270).
94. European Commission, Proposal for a Regulation of the European Parliament on establishing the European Competitiveness Fund ('ECF'), op. cit.
95. European Commission, Communication on The EU Startup and Scaleup Strategy, op. cit., p. 9.
96. https://policy.trade.ec.europa.eu/news/report-highlights-eus-approach-export-controls-dual-use-items-2025-01-31_en.
97. Alavi, H., & Khamichonak, T. (2016). A European dilemma: The EU export control regime on dual-use goods and technologies. DANUBE: Law and Economics Review, 7(3), 161-172.
98. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 19 March 2025 White Paper: For European Defence Readiness 2030, op. cit., p. 4.
99. Ibid., p. 15.
100. Ibid., p. 15.
101. Letta, E. Much More than a Market: Speed, Security, Solidarity. Empowering the Single Market to deliver a sustainable future and prosperity for all EU Citizens, April 2024 (https://www.consilium.europa.eu/media/ny3j24sm/much-more-than-a-market-report-by-enrico-letta.pdf), pp. 13-14.
102. The Draghi report: A competitiveness strategy for Europe, op. cit.
103. Joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 19 March 2025 White Paper: For European Defence Readiness 2030, op. cit., p. 18.
104. Ibidem, p. 18.
105. Ibidem, p. 14.
106. Ibidem, p. 9.

Publisher
28DIGITAL
Rue Guimard 7
1040 Brussels
Belgium
www.28digital.eu

Contact
info@28digital.eu

ISBN 978-91-87253-74-4

28DGTL

Initiated by the European Institute of Innovation and Technology (EIT)