MARKETING OF SCIENTIFIC AND RESEARCH ORGANIZATIONS, 2025, Vol. 57, Issue 3, p. 39–66
pISSN 2353-8503
eISSN 2353-8414

FROM INNOVATION TO ADOPTION: A NARRATIVE SCOPING REVIEW OF DEFENCETECH ECOSYSTEMS, STARTUPS, AND DUAL-USE ACCELERATION MECHANISMS

Yelyzaveta Leshchenko[1], **Justyna Pelc**[2, 3]
[1] PSPA, Polish Space Professionals Association, 16A/41 Edmunda Jana Osmańczyka St.,01-494 Warsaw, Poland
[2] Resquant, 40/1 Narutowicza St., 90-135 Lodz, Poland
[3] New Space Marketing, Warsaw, Poland
[1] E-mail: leshchenkoyp@gmail.com
[1] ORCID: 0009-0008-2254-1779
[2] E-mail: justyna@resquant.com
[2] ORCID: 0009-0003-9138-4379

DOI: 10.2478/minib-2025-0013

ABSTRACT

The study is based on an analysis of existing academic literature, policy documents and industry reports, allowing for a broad understanding of how defence innovation ecosystems function.

The findings show that startups increasingly drive technological progress in areas such as artificial intelligence, autonomy, cyber defence, quantum technologies and space, while facing substantial barriers related to regulation, procurement timelines and access to defence institutions. Investment activity in the sector is expanding but remains constrained by long development cycles and risk profiles, which has encouraged the creation of specialised defence-focused funds. Accelerator programmes support technology adoption by offering structured pathways into defence markets, access to testing environments and closer interaction with military and governmental stakeholders.

The practical implications of the study highlight the need for more adaptive funding mechanisms, improved support for dual-use innovation and stronger public–private cooperation to accelerate technology deployment. The article contributes by offering a clear and accessible synthesis of key factors shaping the DefenceTech landscape and the collaborative dynamics required for its effective growth.

This article adopts a narrative scoping review approach integrating academic and institutional sources to synthesise current knowledge on DefenceTech ecosystems.

Key words: DefenceTech, startups, venture capitals, global security, dual-use.

Type of the work: review article

Article History
Received: February 13, 2026 | **Revised:** April 13, 2026 | **Accepted:** April 14, 2026

1. Introduction

The DefenceTech sector has become a fundamental component of current security and industrial policy (Ilchenko et al., 2021). Key factors contributing to this development include accelerating geopolitical competition, technological shifts, and the growing military relevance of commercially driven innovation (Hajdú, 2025). In the geopolitical landscape, governments and international organisations are increasingly prioritising technologies with both civilian and defence applications. These technologies are being recognised as essential for achieving strategic autonomy, ensuring secure supply chains and maintaining operational advantage. The European Commission formally identifies dual-use research and development as a critical pillar of Europe's technological sovereignty and recommends expanding support mechanisms for such innovation (Publications Office of the EU, 2024).

DefenceTech is defined as the set of technologies and systems employed to strengthen defence capabilities in the domains of intelligence, surveillance, communications, cyber defence, autonomy, space, and advanced sensor or simulation environments. Recent developments in European defence innovation have been dominated by dual-use technologies, including unmanned aerial vehicles (UAV), advanced materials, cyber-security tools, and space-based services. Analyses of European strategic dependencies have demonstrated that dual-use capabilities, including robotics, unmanned systems, additive manufacturing, batteries and semiconductor-based technologies, are imperative for both military readiness and industrial resilience (Blagoeva et al., 2019).

The strategic value of DefenceTech is reinforced by Europe's evolving security environment. Increased great-power competition, the growth of hybrid threats, and escalating military activity in neighbouring regions have caused a shift in defence planning towards faster innovation cycles and greater technological independence (Hajdú, 2025). European legislative assessments emphasise that critical technologies particularly AI, quantum technologies, space technologies, cyber technologies and advanced materials are essential for securing defence readiness and industrial competitiveness (European Commission, 2025b; NATO, 2025c). These assessments also highlight the importance of coordinated industrial investment and stronger public–private cooperation in order to sustain the development of Europe's defence capabilities (European Parliament, 2023).

The defence innovation landscape now relies heavily on commercial technology ecosystems. Major breakthroughs in areas such as autonomy, cybersecurity, machine learning, robotics and advanced computing now originate from startups and SMEs rather than defence prime contractors. Defence institutions are increasingly dependent on civilian innovation pipelines, particularly in areas with dual-use potential. Analyses at parliamentary and alliance level confirm that many technologies essential for military

modernisation first emerge in commercial markets before being adapted for operational use, thus reversing the historical direction of innovation in the defence sector (NATO Parliamentary Assembly, 2024).

NATO's technology policy frameworks also emphasise the importance of incorporating startups, SMEs and up-and-coming tech companies into defence capability development. Alliance-level initiatives outline mechanisms for accelerating the adoption of technologies, improving procurement processes and enabling a faster transition into operational use. The 2025 Rapid Adoption Action Plan recognises innovation ecosystems as a structural requirement for maintaining technological advantage, encouraging closer collaboration between defence authorities, the private sector, and academia (NATO, 2025b).

Despite the growing number of institutional reports and policy analyses on DefenceTech innovation, existing literature remains fragmented and often lacks an integrated analytical perspective on how startups, venture capital and acceleration mechanisms jointly shape defence innovation ecosystems.

This article therefore addresses the following research question: How do startups, financing mechanisms, and acceleration instruments jointly shape technology adoption pathways within DefenceTech innovation ecosystems, and what structural barriers constrain this process? The study aims to synthesise available academic and institutional evidence on these dynamics in order to identify the key enabling and constraining factors for defence innovation adoption in the European and transatlantic context.

To structure the analytical framework of this study, the research examines four interrelated dimensions of DefenceTech innovation ecosystems: the structural and institutional barriers influencing ecosystem functioning, the evolving roles of startups as key innovation actors, the impact of financing models and acceleration mechanisms on innovation pathways, and the ecosystem-level collaboration processes shaping the adoption of emerging defence technologies.

2. Methodology of the Review

This article is designed as a narrative scoping review combining peer-reviewed academic literature with institutional and policy documents (grey literature). The aim of this review is to synthesise existing knowledge on DefenceTech innovation ecosystems, focusing on the interaction between startups, financing mechanisms and acceleration instruments, and to identify structural barriers and enabling factors shaping technology adoption.

This study applies a narrative scoping review approach aimed at synthesising dispersed academic and institutional knowledge. The review primarily covers materials published

between 2019 and 2026. Key search terms included: "Defence Technology ecosystem", "Defence innovation ecosystem", "dual-use innovation", "defence startups", "military innovation accelerators", and "defence venture capital".

Sources included peer-reviewed academic publications and institutional reports (EU, NATO, RAND, SIPRI, ESA, OECD). Grey literature was included due to the policy-driven nature of defence innovation. Materials were selected based on relevance to innovation ecosystems, financing mechanisms, institutional barriers and technology adoption. Media commentary and purely technical engineering studies were excluded.

The analysis followed a thematic synthesis approach structured around recurring themes such as procurement constraints, investment dynamics, interoperability requirements and acceleration mechanisms.

3. DefenceTech Ecosystem Context

3.1. Key DefenceTech domains

Institutional analyses and strategic reports indicate that the development of DefenceTech in the European Union and globally is increasingly focused on a limited number of technological areas considered key to future military capabilities. The most frequently identified areas include artificial intelligence, unmanned systems, cybersecurity and electronic warfare, space technologies, microelectronics, and quantum technologies (European Commission, 2025a).

The RAND Corporation report indicates that in the short and medium term, the most important military applications of artificial intelligence relate to data analysis, intelligence, surveillance, and reconnaissance (ISR), logistics optimization, and decision support systems, with the analysis focusing on the impact of AI on the conduct of military competition rather than on a detailed assessment of specific categories of autonomous strike systems (RAND Corporation, 2026). In this context, AI is seen primarily as a tool for increasing the speed and quality of decision-making through the fusion of sensor data, predictive analysis, and improved situational awareness (NATO, 2024).

In the European Union, a similar approach can be seen in the structure of projects financed under the European Defence Fund, where the use of artificial intelligence focuses mainly on command and control systems, operational data analysis, and planning support (European Commission, 2025c). Similar priorities are identified in the strategic documents of the US Department of Defense, which emphasize the responsible use of AI, the need for human oversight, and the pursuit of decision-making advantage rather than full autonomy of combat systems (U.S. Department of Defense, 2022).

Unmanned systems (UAVs, UGVs, USVs) are widely identified as one of the key areas of development for DefenceTech. However, analyses by the International Institute for Strategic Studies emphasize that their operational effectiveness depends primarily on the degree of integration with command, communications, and electronic warfare systems, and not solely on the technical parameters of the platform itself (International Institute for Strategic Studies (IISS), 2024).

Experience from the conflict in Ukraine, analyzed by SIPRI, among others, shows that unmanned systems can significantly influence the course of combat operations, while being highly vulnerable to electronic jamming, countermeasures, and rapid cycles of technological adaptation on both sides of the conflict (Stockholm International Peace Research Institute, 2025). In the European Union, the development of these technologies focuses mainly on reconnaissance, logistics, and security applications, which is reflected in the portfolios of projects financed by the European defence Fund and the European defence Agency (European Defence Agency, 2023a).

Publications by the NATO Cooperative Cyber Defence Center of Excellence indicate that a significant portion of cyber threats in the military environment are related to the software supply chain, including commercial components integrated into defence systems (NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2024). Consequently, DefenceTech development in this area focuses on increasing the resilience of command and control systems, securing the software supply chain, and integrating cyber defence and electronic warfare capabilities into multi-domain operations (U.S. Department of Defense, 2023).

The Space Threat Assessment 2024 report prepared by the Center for Strategic and International Studies indicates that satellite systems, particularly those in low Earth orbit (LEO), are playing an increasing role in military communications, navigation, and reconnaissance capabilities, while at the same time becoming more vulnerable to interference, cyberattacks, and counter-space activities (Center for Strategic and International Studies (CSIS), 2024).

In the European Union, space-related defence technology includes the development of Earth observation systems, secure satellite communications, and navigation services, carried out under European Union programs and in cooperation with the European Space Agency (European Space Agency, 2024). At the same time, SIPRI analyses indicate that space has become an area of intensifying strategic competition between major international actors (Stockholm International Peace Research Institute, 2024b).

A special report by the European Court of Auditors indicates that limited access to advanced microelectronics is one of the key constraints on the development of modern DefenceTech systems in the European Union (European Court of Auditors, 2025).

Semiconductors are a critical component for systems based on artificial intelligence, radar, electronic warfare, and autonomous platforms, which means that their availability has a direct impact on operational capabilities.

Quantum technologies remain at a relatively early stage of development for military applications. UNIDIR analyses indicate that the most realistic short-term applications are in quantum sensing and precision measurement systems, while quantum communication and cryptography are seen as a long-term prospect (United Nations Institute for Disarmament Research (UNIDIR), 2024). At the same time, the EU, the US, and China treat quantum technologies as part of long-term technological competition, which is reflected in strategic documents and research and development programs (RAND Corporation, 2024).

4. Ecosystem Actors in DefenceTech Innovation

Defence innovation ecosystems are often described as structured around three interdependent pillars: military science, industrial capabilities and defence requirements, whose interaction determines the direction and effectiveness of technological development (Hajdú, 2025).

DefenceTech innovation ecosystems consist of several interdependent actor groups whose roles shape both technological development and adoption pathways. Startups operate as key sources of innovation, particularly in software, autonomy and cyber capabilities, where rapid iteration cycles contrast with the longer development timelines of traditional defence contractors. Qualitative ecosystem studies based on twenty-six semi-structured interviews further indicate that startups increasingly shape defence innovation trajectories despite structural entry barriers related to procurement and regulatory complexity (Atkinson, 2025).

Venture capital investors increasingly influence the sector by introducing scaling logics and risk models derived from the commercial technology domain, which affects procurement expectations and growth strategies.

Defence industrial ecosystems are structured as multi-tier supply networks in which prime contractors depend on extensive layers of specialised suppliers and SMEs, illustrating how innovation emerges through vertically integrated yet interdependent actor relationships rather than isolated firm-level capabilities (Heidenkamp et al., 2011). Defence institutions and prime contractors remain dominant demand-side actors, as access to testing infrastructure, certification procedures and acquisition programmes largely determines whether new technologies transition from experimentation to operational deployment.

In parallel, accelerators and publicly supported innovation programmes function as intermediary actors that reduce coordination barriers between emerging firms and military stakeholders, supporting early validation and ecosystem integration. Comparative analyses of defence innovation intermediaries indicate that newly established organisations already replicate seventeen out of twenty functional roles traditionally performed by commercial innovation intermediaries, reinforcing their systemic role as boundary-spanning actors within emerging defence innovation ecosystems (Schmid & Wong, 2020). Research on asymmetric innovation partnerships demonstrates that defence innovation ecosystems evolve through iterative collaboration between large integrators and startups, where empirical learning cycles continuously reshape value creation and capability development processes (Graarud & Kristensen, 2025).

Together, these actors form a structured innovation environment in which institutional constraints, financing mechanisms and collaboration formats co-evolve rather than operate as isolated drivers of change. Empirical ecosystem research based on longitudinal data from 4,903 investor–investee relationships shows that technological alliances within an ecosystem can positively influence venture performance, highlighting the importance of interdependent actor networks in innovation ecosystems (Chen et al., 2024). Comparative defence innovation research analysing seven national innovation systems demonstrates that technological advantage emerges from interactions between state institutions, industry and scientific actors rather than from isolated technological breakthroughs (Cheung, 2021).

Types of DefenceTech startups

Startups have become a key driver of technological innovation in the DefenceTech sector, particularly in areas where rapid experimentation, iterative development and high-risk technological exploration offer an advantage over traditional defence industrial models. Their growing importance reflects a global shift in defence innovation dynamics, whereby emerging capabilities largely originate from the commercial and dual-use sectors rather than from conventional defence contractors. This trend is evident across Europe and NATO, where strategic documents consistently recognise startups as major contributors to emerging and disruptive technologies, including artificial intelligence, autonomous systems, quantum technologies, cybersecurity, and next-generation space systems (NATO, 2025b).

DefenceTech startups can be broadly categorised according to their technological focus and operating model. Hardware-oriented startups develop physical systems such as

drones, autonomous ground vehicles, robotic platforms, sensors, novel materials, energy systems or small satellites. Such ventures typically require substantial capital, access to testing environments and lengthy prototype cycles. Structural barriers within DefenceTech ecosystems also exhibit a strong spatial dimension. Empirical analyses indicate that approximately 85% of Defence Innovation Ecosystem startups are concentrated in urban innovation hubs, while only 15% operate in peripheral regions, limiting access to testing infrastructure, institutional networks and defence stakeholders outside core ecosystem locations (Kondrats et al., 2025). Their importance is emphasised by Europe's need to enhance its capabilities in critical supply chain areas such as advanced manufacturing, semiconductors, power systems, and space technologies (European Commission, 2024a).

Software-oriented startups are focusing on digital capabilities, including cyber defence tools, command-and-control systems, AI-based decision support systems, data fusion platforms, and simulation technologies (Schwarz, 2025). These ventures are one of the fastest-growing segments in the sector as defence institutions are becoming increasingly dependent on flexible and scalable digital infrastructures (European Commission, 2021). Assessments of critical technologies for European defence identify advanced software and AI capabilities as vital for operational readiness, resilience and situational awareness (European Parliament, 2023).

A third group consists of dual-use startups whose technologies originate in civilian markets but have strategic defence applications. These include companies specialising in robotics, Earth observation analytics, cybersecurity, digital twins, telecommunications, advanced materials, energy storage and autonomous mobility. The European Commission's 2024 White Paper identifies these firms as being crucial to Europe's long-term technological sovereignty, as dual-use innovation frequently surpasses traditional defence R&D, enabling the military to adopt commercial technologies more efficiently (European Commission, 2024d).

Building on the typology of DefenceTech startups discussed earlier (hardware-focused, software-driven and dual-use ventures), Table 1 links the structural barriers they face with governance instruments and resulting ecosystem-level effects.

Table 1. Typology of DefenceTech startups and ecosystem implications for financing, market entry, and adoption.

Startup category	Core technological focus	Financing profile	Key ecosystem barriers	Primary market entry pathway	Implications for defence adoption
Hardware-oriented startups	UAVs, robotics, advanced sensors, space systems, materials	Capital-intensive; mixed public funding and specialised VC	Certification, testing infrastructure, procurement timelines	Subcontracting to primes, pilot defence projects	Slower adoption but strong impact on capability development
Software-oriented startups	AI, cyber defence, data fusion, C2 platforms, simulation	Venture capital-driven with dual-use scaling	Security accreditation, interoperability standards	Integration into digital architectures and defence platforms	Accelerates operational decision-making and system integration
Dual-use startups	Space analytics, telecom, autonomy software, digital twins	Hybrid financing (EIC, VC, public–private funds)	Export controls, regulatory fragmentation	Transition from civilian markets to defence programmes	Enables rapid innovation transfer but requires institutional mediation

5. Innovation Financing and Acceleration Mechanisms

5.1. Public and Private Funding Instruments

The financing of innovation in the defenceTech sector is currently undergoing significant change, driven by the growing role of the dual-use approach and the need for shorter technology development cycles. Traditional defence procurement models were based mainly on large public contracts, while the modern financing ecosystem includes venture capital, specialized funds, European Union instruments, and national programs targeting startups and SMEs (European Commission, 2023).

The growing activity of venture capital funds in the DefenceTech sector is directly related to the convergence of civil and defence innovations, particularly in the areas of artificial intelligence, cybersecurity, and space technology. Corporate venture capital plays

the role of an intermediary between startups and the traditional defence industry in this process, offering access to technological infrastructure and testing environments that enable early validation of solutions (European Commission, 2025d). Investments in DefenceTech are characterized by higher regulatory risk and a longer return horizon than classic deep-tech, which affects the structure of financing rounds and the participation of the state as a co-investor.

In response to the need for faster absorption of strategic technologies, specialized investment funds are being created. Public–private financing mechanisms increasingly shape DefenceTech ecosystems, as illustrated by the NATO Innovation Fund, a €1 billion multilateral venture capital initiative designed to invest in dual-use startups and accelerate technological scaling across allied innovation networks in areas such as AI, quantum computing, and autonomy (NATO Innovation Fund, 2026). The In-Q-Tel model, on the other hand, shows that strategic funds can act as the first technology customer, accelerating the commercialization of solutions developed by young technology companies (In-Q-Tel, 2026).

At the European Union level, the European defence Fund (EDF) remains a key support instrument, financing research and development projects carried out by international industrial and technological consortia. The EDF increases the participation of startups through requirements for SME participation and financing of high-risk technologies, which often do not receive private support in the early stages of development (European Commission, 2026). The EDF is complemented by civilian instruments such as the European Innovation Council, which enable the financing of deep tech with dual-use potential and provide startups with a pathway into defence projects (European Innovation Council, 2026).

The result is a hybrid model of DefenceTech financing, combining public grants, VC investments, and pilot contracts, in which the return on investment is often strategic in nature, related to technological resilience and industrial autonomy, rather than solely to financial gain. European policy analyses emphasise that dual-use innovation ecosystems increasingly rely on SMEs, startups and scale-ups operating across civil–defence boundaries, reflecting a shift from traditional defence-only innovation models toward hybrid ecosystem structures (European Commission, 2024c).

5.2. Acceleration programs and support instruments

In response to the problem of the defence sector's limited capacity to rapidly absorb technological innovations, new mechanisms for accelerating and adopting innovations have been initiated, with the aim of shortening the gap between technological development and its potential use in the security and defence environment.

At the alliance level, one of the key new instruments is NATO DIANA (Defence Innovation Accelerator for the North Atlantic) (NATO, 2026). According to NATO documents, DIANA was established in response to the need to systematically integrate civilian innovators into the defence ecosystem and to test technologies considered critical to the Alliance's security, such as artificial intelligence, autonomy, space technologies, system resilience, new materials, and energy (NATO, 2025a). The program focuses on working with innovators in the early stages of technology development and creating conditions for their pilot validation. Selected projects gain access to a network of accelerators and testing infrastructure, allowing for early assessment of their operational suitability without launching full procurement procedures (NATO, 2026). This mechanism aims to shorten the time needed to identify technologies with military potential and reduce the risks associated with their further development.

The DIANA architecture design includes test environments referred to as Living Labs. According to NATO implementation documents, the first pilot Living Lab is currently being launched, enabling technology validation in conditions similar to operational ones and direct interaction with military users (NATO, 2026). These solutions are intended to support the transition from technology demonstration to its potential adoption within NATO structures, especially in areas where the pace of civilian technology development significantly exceeds that of traditional armament programs.

DIANA's activities are linked to the Alliance's transformation processes coordinated by NATO Allied Command Transformation, which is responsible for integrating the findings of technological experiments into NATO doctrine, training, and exercises. ACT ensures the consistency of innovation with long-term capability planning (NATO Allied Command Transformation, 2025).

At the European Union level, the European defence Innovation Scheme (EUDIS), established under the European defence Industrial Strategy, is the framework instrument supporting defence innovation. According to European Commission documents, EUDIS aims to increase the EU's capacity to absorb defence innovation by coordinating activities in the areas of technology testing, interoperability, and the inclusion of new entities, in particular startups and SMEs, into the European defence ecosystem (European Commission, 2025a).

Space technologies are also an important component of this ecosystem. ESA Business Incubation Centers serve as incubators for space startups and are not defence programs or formally focused on dual-use technologies (European Space Agency, 2026). At the same time, the European Space Agency consistently points out that technologies developed within space programs, in particular Earth observation, satellite navigation, secure communications, and satellite data analysis, are key components of modern security and

defence capabilities, including situational awareness and critical infrastructure resilience. In this context, the announcement of the creation of a new ESA center in Poland, focused on security and dual-use technologies, is also significant. According to ESA communications, this initiative is intended to complement the Agency's existing instruments and strengthen the development of technologies relevant to national security and systemic resilience, without replacing the ESA BIC network (European Space Agency, 2023).

In addition to allied and EU initiatives, national acceleration programs and rapid technology adoption mechanisms, which often feature greater procedural flexibility and stronger links to end users, play an important role in the DefenceTech ecosystem.

In the United Kingdom, this function is performed by the Defence and Security Accelerator (DASA), which operates on the basis of so-called themed calls and problem-led competitions. This mechanism enables the testing of technologies in response to the specific operational needs of the Ministry of Defence, as well as the conduct of pilot projects and demonstrations in close cooperation with the military and security services (UK Ministry of Defence, 2026).

In France, a similar role is played by the Agence de l'innovation de défense (AID), operating within the structures of the Ministry of the Armed Forces. The AID integrates acceleration, experimentation, and dialogue with military users into a single institutional process, which allows for rapid testing of technologies and their adaptation to French operational needs (French Ministry of Armed Forces, 2026).

The analysis indicates that the problem of the DefenceTech sector's limited capacity to absorb innovation has been clearly recognized at the allied, EU, and national levels. In response, initial steps have been taken in the form of acceleration programs and technology testing and adoption instruments, such as NATO DIANA, EUDIS, and selected national mechanisms. However, these initiatives should be seen as the initial stage in the process of building a more coherent defence innovation system.

5.3. Ecosystem collaboration

The development of DefenceTech is becoming increasingly dependent on the coordinated cooperation of public authorities, the armed forces, industry, research institutions, and private technology firms. Defence innovation ecosystems are multilayered structures in which each stakeholder contributes capabilities that no single entity can provide alone. Governments and public administrations play a foundational role in this ecosystem by defining strategic priorities, setting regulatory frameworks, financing early-stage research and development (R&D) and shaping long-term industrial policies. European and NATO-level strategies emphasise the need for state institutions to

ensure continuity of investment in emerging and disruptive technologies, reduce regulatory fragmentation and create targeted instruments to support dual-use and defence innovation (European Commission, 2024d).

DefenceTech ecosystems rely heavily on armed forces due to their specialised operational expertise, specific capability needs and access to authentic testing environments. Defence organisations provide mission-based feedback that is essential for validating technology in areas such as autonomy, cyber defence, situational awareness, data fusion, advanced sensors and robotics. NATO's strategic analyses identify structured military–technology interaction as a decisive enabler of EDT maturity and operational adoption, particularly where testing, certification and iterative co-development are required (Fertasi, 2019). The armed forces also contribute to standardisation, doctrine integration and long-term capability planning, making them an indispensable partner for startups and private firms seeking to align their innovations with defence requirements (NATO, 2025b).

The industry, comprising both defence contractors and emerging technology companies, provides the necessary production capacity, supply chain infrastructure, and system integration capabilities to translate prototypes into scalable, deployable systems. While traditional defence companies remain essential for highly complex platforms such as aircraft, naval systems, advanced communications and integrated command networks, startups and SMEs contribute agility and specialised technological breakthroughs. Analyses of European defence innovation emphasise that industrial cooperation must leverage these complementary strengths to accelerate the adoption of critical technologies, including AI, quantum technologies, advanced materials, and space systems (European Parliament, 2023).

The formation of DefenceTech ecosystems is now primarily organised through public–private partnerships (PPPs). These partnerships facilitate co-investment and co-development, as well as providing shared access to expertise, infrastructure, and testing environments (Fertasi, 2019). They also enable risk-sharing between governments and private actors, which is particularly important in early-stage technological domains that require long development cycles and significant capital. The European Commission and the Joint Research Centre emphasise the structural requirement of PPPs for reducing Europe's dependency on external technologies and for strengthening domestic capabilities across critical sectors, including semiconductors, robotics, cybersecurity, materials, and energy systems (Liwång, 2022).

At the operational level, defence innovation ecosystems are becoming more dependent on innovation hubs, accelerators, co-creation facilities and test ranges, which bring together military users, researchers, startups and industry. NATO's innovation framework

encourages the creation of integrated environments in which technology developers can experiment, receive cross-domain feedback, and adapt solutions progressively for deployment (Fertasi, 2019). The importance of such ecosystems is consistently emphasised in alliance-level analyses of emerging and disruptive technologies, which highlight the strong correlation between EDT adoption and the availability of shared testing infrastructure, open innovation channels and structured public–private collaboration (NATO, 2025c).

These ecosystems also facilitate knowledge transfer between civilian and defence sectors. Dual-use technologies often originate in commercial markets, yet their successful adaptation for defence applications requires operational validation, cybersecurity hardening, compliance with defence standards and integration into military systems architectures. Innovation ecosystems therefore function as translation mechanisms that connect fast-paced commercial R&D with the stringent technical and security requirements of defence institutions. Recent DoD initiatives such as the TRL Bootcamp pilot launched in March 2024 illustrate institutional attempts to bridge the transition gap between early-stage funding mechanisms and operational defence programs, highlighting systemic challenges in technology maturation pathways (Doumitt et al., 2025).

Long-term capability planning in Europe further highlights the increasing requirement for systemic cooperation. European defence policy frameworks advocate coordinated national and EU-level action to enhance industrial resilience, support cross-border defence supply chains, and align technology development priorities among member states. These policies emphasise that DefenceTech innovation cannot rely exclusively on market forces, but rather requires active collaboration between the public and private sectors to guarantee sovereignty over vital technologies and maintain competitiveness in emerging fields.

In practice, effective cooperation within ecosystems leads to the accelerated adoption of technology, reduced development risk, improved interoperability, and stronger strategic autonomy. Thus, DefenceTech ecosystems operate not just as collections of independent actors, but as interdependent networks in which administrations define strategic direction, armed forces provide operational insight and industry transforms emerging technologies into deployable capabilities. Public–private partnerships, shared testing infrastructures, and coordinated innovation frameworks create an environment that enables DefenceTech to grow and deliver long-term security and technological advantages (Ilchenko et al., 2021).

6. Structural and Institutional Barriers in DefenceTech Ecosystems

Despite growing strategic importance, DefenceTech startups face a unique and complex set of development challenges. Long procurement cycles pose a significant barrier to early growth, as defence institutions typically require multi-year validation, certification and budgeting procedures before acquiring new technologies. Studies of ten early-stage dual-use hardware startups reveal hybrid financing patterns combining federal grant funding with venture capital investment, reflecting the increasing convergence between public innovation programs and private capital within DefenceTech ecosystems (Amir & Rombach, 2025). Analyses of defence technology transition processes indicate that moving from prototype development to operational deployment frequently requires five to seven years, reinforcing the systemic mismatch between rapid technological innovation cycles and institutional acquisition timelines (Naval Postgraduate School, 2020a). Analyses of national security innovation systems emphasise that commercial innovation ecosystems prioritise accelerated development cycles and rapid scaling, creating structural tensions when these dynamics interact with slower defence procurement processes (Wilson, 2024). This contrasts with commercial markets, where shorter sales cycles and broader customer bases enable faster revenue generation. Parliamentary and alliance-level analyses consistently highlight that slow procurement processes limit the deployment of emerging technologies and reduce smaller firms' ability to scale (NATO Parliamentary Assembly, 2024).

Further barriers to entry are raised by regulatory and compliance requirements. Export controls, security clearances, data-handling rules and defence-specific certification standards impose administrative and financial burdens that many early-stage ventures find difficult to meet. Recent defence industry analyses highlight that the rapid proliferation of innovation pathways, accelerators and acquisition mechanisms has created a complex institutional landscape that many non-traditional vendors struggle to navigate effectively (Carberry, 2023). In practice, security clearance procedures may extend up to 18 months even for experienced defence suppliers, significantly increasing entry costs for startups and slowing the transition from prototype development to operational deployment (Andersson, 2022). These constraints are particularly challenging for dual-use companies operating in both commercial and defence markets, as they must navigate the complex intersection of regulations affecting product design, manufacturing, talent recruitment, and international expansion. The European Commission is aware of these challenges and has recommended reforms to encourage cross-border innovation and reduce regulatory fragmentation in Europe's dual-use sector (European Commission, 2024d).

Access to testing environments, military users and mission-specific data also affects the development of startups. Many emerging technologies, such as autonomous navigation, sensing, space situational awareness and cyber defence, cannot be validated without realistic operational conditions. Defence institutions are working to expand test ranges, sandboxes and innovation hubs, but significant gaps remain, particularly for early-stage companies lacking institutional partnerships. Technological trend analyses consistently highlight the need for expanded testing infrastructures, emphasising real-world operational validation as a critical requirement for EDT maturity (NATO, 2025c).

Financing remains another structural challenge. Large-scale ecosystem studies based on 411,389 patents indicate that innovation success is strongly shaped by institutional ecosystems involving universities, research organisations and public subsidies, while SMEs tend to play a more limited role in patent performance outcomes (Stasik, 2026). Hardware-intensive DefenceTech ventures require significant capital, while software and dual-use firms often find it difficult to persuade traditional investors to fund defence applications due to perceived political, ethical or market-related risks (RAND Corporation, 2026). Empirical analyses of early-stage dual-use hardware ventures examining ten strategically important startups highlight the growing reliance on mixed financing structures combining public funding instruments and venture capital within DefenceTech ecosystems (McLeod, 2022). Interviews with venture capital actors highlight that European defence innovation ecosystems still face capital allocation imbalances, with public funding frequently directed toward established prime contractors rather than SMEs and early-stage startups (Atkinson, 2025).

Analyses of the European and transatlantic defence innovation landscape emphasise the persistence of investment gaps, particularly in the case of early-stage hardware ventures. These analyses also highlight the need for specialised public–private funds to close these gaps and enable scaling (European Parliament, 2023). Data-driven analyses of dual-use startup ecosystems based on SBIR and STTR programme datasets further demonstrate that structured public innovation programmes significantly influence long-term scaling trajectories and survival rates of emerging defence technology ventures (Ying, 2025). Structural capability differences remain significant, as policy analyses indicate that EU27 countries spend approximately seventeen times less on defence research and development than the United States, shaping the scale and tempo of European DefenceTech innovation ecosystems (European Commission, 2024c).

Finally, scaling up DefenceTech startups requires establishing trust and long-term relationships with defence institutions. Interview-based ecosystem research further emphasises that limited access to networks, unpredictable procurement timelines and financing gaps collectively constrain startups' ability to scale within defence markets (Amir

& Rombach, 2025). This sector places a high value on reliability, security, compliance and operational continuity. startups must therefore deliver both technological innovation and institutional credibility, which requires structured engagement with defence users, rigorous certification processes, stable financing and long-term product roadmaps.

7. Structural and Institutional Barriers in DefenceTech Ecosystems

The structural barriers discussed in the previous section highlight the constraints faced by DefenceTech startups at the organisational level. Building on this perspective, the following analysis shifts towards the ecosystem scale, examining how institutional frameworks, regulatory regimes and policy instruments shape broader innovation dynamics. Rather than presenting additional barriers, export control systems, procurement architectures and security standards are analysed here as governance mechanisms that structure technological development, market access and collaboration patterns across the DefenceTech ecosystem.

At the ecosystem level, the rapid development of disruptive technologies such as artificial intelligence, autonomous systems, space and quantum technologies, and advanced communications systems has fundamentally changed the nature of defence and the relationship between the state, industry, and the innovation ecosystem. Process-oriented analyses of defence innovation emphasise that technological development should be understood as a continuum from early research to operational impact, embedded within stakeholder-driven innovation ecosystems rather than isolated organisational efforts (Carberry, 2023). The NATO Strategic Concept adopted in 2022 clearly indicates that emerging and disruptive technologies (EDTs) are both a source of new opportunities and significant risks to security, changing the nature of conflict and becoming one of the key areas of global competition (NATO, 2022). This structural dynamic is reinforced by the absence of formalised rapid acquisition mechanisms, which contributes to the so-called "valley of death" between technology demonstration and operational procurement identified by the European Commission (European Commission, 2025a).

The ecosystem dynamics described above are synthesised in Figure 1, which illustrates the multi-actor structure of the DefenceTech environment, the flow of capital between public and private stakeholders, and the critical transition points between research, testing, and operational deployment.

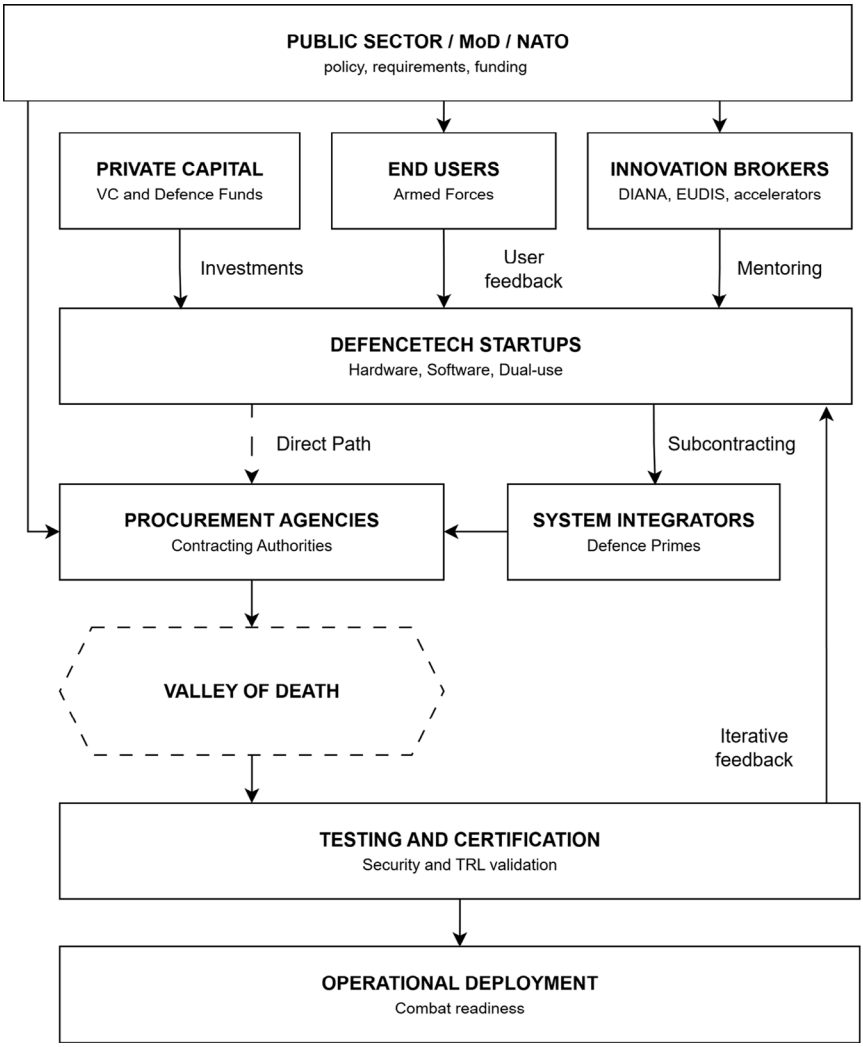

Figure 1. DefenceTech ecosystem from institutional oversight to operational adoption.

DefenceTech is a specific segment of the innovative economy in which the pace of technological development is strongly determined by institutional and regulatory factors (European Parliamentary Research Service, 2024b). Foresight-oriented defence policy analyses also emphasise that flexibility across multiple operational domains has become a central design principle shaping contemporary military innovation ecosystems. Rather than focusing on single-domain superiority, future capability planning increasingly prioritises adaptable and multi-role systems capable of operating across land, air, sea, cyber and space environments, reinforcing ecosystem-based approaches to defence

innovation (Oitaku, 2021). Empirical analyses of 63,714 defence-related inventions show strong ecosystem concentration, with the twenty largest organisations accounting for around 40% of total innovation output and approximately 41% of inventions exhibiting dual-use characteristics, highlighting the structural dominance of key actors within DefenceTech innovation systems (Caviggioli, 2018).

Unlike civilian deep tech sectors, the successful implementation of innovation in the defence sector depends not only on the maturity of the technology, but also on its ability to pass through the public procurement system, security requirements, and export controls. At the ecosystem level, defence innovation trajectories are structured by regulatory regimes, procurement architectures and interoperability requirements.

The British Ministry of Defence's industrial strategy indicates that the average time for a new supplier to enter the defence sector is a lengthy process fraught with significant procedural barriers. It is important to note that a key part of this period is taken up by procedures not directly related to technology development. These include, in particular, security certification of personnel and facilities, accreditation of IT systems, and complex and time-consuming public procurement procedures (UK Ministry of Defence, 2025). The document emphasizes that these barriers are institutional in nature and remain largely independent of the level of innovation of the solution offered.

At the same time, data from the Stockholm International Peace Research Institute (SIPRI) indicate a very high level of revenue concentration in the global arms industry. According to the SIPRI Top 100 arms-producing and military services companies ranking, the total sales value of the 100 largest arms and military services manufacturers amounted to approximately USD 679 billion (Stockholm International Peace Research Institute, 2024a). Based on individual data published by SIPRI, it can be concluded that the ten largest companies generate approximately 50% of the total revenues of this group, which indicates a strong economic concentration among the largest entities in the sector. Longitudinal procurement data show that the number of unique Department of Defense suppliers declined from 79,993 in 2010 to 51,239 in 2019, while first-time vendors dropped from over 15,000 to just above 4,200, illustrating increasing structural barriers to entry within defence innovation ecosystems (Naval Postgraduate School, 2020b).

SIPRI emphasizes that this market structure favors the consolidation of dominant companies that have economies of scale, the ability to integrate complex weapons systems, and long-term relationships with public administrations. As a result, new entrants, including startups and small and medium-sized enterprises, most often enter the defence sector as subcontractors or suppliers of specialized components and technologies, rarely acting as prime integrators of complete system capabilities (Stockholm International Peace Research Institute, 2024b).

As a governance instrument, export control remains the responsibility of EU member states, shaping market structure and influencing cross-border innovation pathways within the DefenceTech ecosystem (In-Q-Tel, 2026). Policy analyses of the European Defence Technological and Industrial Base emphasise persistent fragmentation and limited cross-border collaboration, which structurally constrain innovation scaling across the ecosystem (Knudsen et al., 2025). The EU export control regime classifies technologies such as autonomous systems, advanced sensors, semiconductors and cyber tools as dual-use goods if they meet specific technical criteria (European Union, 2021), which results in licensing procedures, restrictions on knowledge transfer and regulatory fragmentation across national jurisdictions. Analyses by the European Parliamentary Research Service indicate that export control procedures may significantly extend commercialization timelines and influence technological design decisions already at the development stage, thereby structuring the conditions under which innovation emerges and scales across the European defence ecosystem (European Parliamentary Research Service, 2024c).

At the ecosystem level, multi-year procurement cycles identified by the European Parliamentary Research Service and the European Defence Agency function as institutional mechanisms that structure capability development timelines and innovation trajectories (European Parliamentary Research Service, 2024a). Procurement processes in the European Union, measured from the identification of an operational need to the achievement of full combat capability, often extend over many years and reflect the sequential nature of planning, financing and implementation of armament programmes. Public procurement based on capability-driven planning promotes interoperability, doctrinal alignment and stability in defence capability development, but simultaneously shapes the pace at which breakthrough technologies can be integrated into operational environments (European Defence Agency, 2023b). EPRS analyses indicate that the absence of formalised rapid acquisition mechanisms influences the absorption of solutions based on artificial intelligence, autonomy and cybersecurity, contributing to systemic gaps between technological experimentation and operational deployment (European Parliamentary Research Service, 2025).

High security requirements operate as institutional safeguards that structure knowledge exchange and collaboration patterns within defence innovation ecosystems. Industrial security requirements in the defence sector cover not only the end product, but also personnel, IT infrastructure, physical facilities, and organizational processes (UK Cabinet Office, 2024). In practice, this means that DefenceTech projects may be subject to partial classification as early as the research and development stage, which significantly limits the possibility of cooperation with universities, civilian startups, and international research partners.

NATO documents indicate that the lack of interoperability of systems using artificial intelligence and autonomy is one of the key operational risks for multinational forces (NATO, 2012). Compliance with standards for command and control (C2) systems, data exchange, and cybersecurity is considered a key eligibility and evaluation criterion for projects in NATO innovation programs and related funding mechanisms (NATO, 2026). At the same time, NATO standardization documents emphasize that the integration of systems after the development phase is a costly, technically difficult process with high operational risk, which justifies the need to consider interoperability already at the design stage (NATO Standardization Office, 2024).

An analysis of the European Defence Fund's results indicates that, in practice, financing is mainly focused on research and development projects at medium levels of technological readiness (typically TRL 3–6), with no mechanism for automatic transition to operational procurement (European Commission, 2025c). The European Commission identifies the so-called "valley of death" between technology demonstration and procurement as one of the key systemic barriers limiting the real impact of innovation on defence capabilities (European Commission, 2025a).

Table 2 synthesises the structural barriers identified in Section 6 with the governance instruments discussed in Section 7, highlighting their combined effects on DefenceTech ecosystem dynamics.

Table 2. Structural barriers, governance instruments and ecosystem-level effects in DefenceTech.

Structural barrier	Governance instruments / interventions	Ecosystem-level effects
Regulatory and compliance requirements	Dual-use regulation, certification standards, export control regimes	Increased administrative burden, delayed market entry, technology design shaped by regulatory constraints
Security and information protection requirements	Security accreditation, classified R&D programmes, controlled-access innovation environments	Limited knowledge exchange, reduced collaboration with civilian actors, slower technology iteration
Defence procurement cycles	Capability-based planning, acquisition procedures, testbeds and innovation programmes	Mismatch between innovation speed and acquisition timelines, "valley of death", low absorption of emerging technologies

Export control and market fragmentation	National licensing systems, EU coordination efforts, alliance-level governance	Restricted cross-border scaling, fragmented markets, regulatory influence on technology architecture

8. The future of the DefenceTech

The future of the DefenceTech sector will be shaped by the rapid development of breakthrough technologies, in particular artificial intelligence, autonomous systems, cybersecurity, space technologies, and, in the longer term, quantum technologies.These technologies increasingly emerge from civilian innovation ecosystems characterised by shorter development cycles, creating a persistent gap between technological advancement and the capacity of defence institutions to absorb new solutions. Both NATO and the European Union identify this gap as one of the key challenges for future defence readiness and technological superiority (European Commission, 2025d; NATO, 2025a).

In response to these trends, models of accelerated technology adoption, including accelerators, pilot programs, test environments, and early operational validation mechanisms, are gaining strategic importance. Rather than functioning solely as support instruments, these mechanisms increasingly act as governance tools that shorten the pathway from experimentation to potential deployment and reduce systemic investment risk. OECD analyses indicate that such solutions serve as "institutional testing grounds," enabling the testing of new models of cooperation with the market and increasing the public sector's capacity to absorb technologies developed outside the traditional industrial base (Organisation for Economic Co-operation and Development, 2024).

An important element of the future DefenceTech ecosystem will be the growing role of startups and SMEs, particularly in the areas of AI, cyber, and space. Recent ecosystem studies indicate that startups increasingly occupy niche roles within defence capability development due to faster innovation cycles compared to traditional contractors (Amir & Rombach, 2025). EU white papers and reports emphasize that these entities are a key source of innovation, but at the same time they most often encounter barriers related to procurement procedures, export regulations, and the lack of stable paths from demonstrator to production contract. Without addressing these structural constraints, publicly funded innovation risks remaining confined to pilot stages rather than translating into deployable defence capabilities (European Commission, 2025d; European Commission, 2024b).

From an ecosystem perspective, the findings suggest that accelerated experimentation frameworks, closer alignment between innovation instruments and capability planning,

and stronger coordination at allied and EU levels are likely to shape future DefenceTech governance trajectories. DefenceTech is therefore increasingly framed not only as an industrial sector but as a systemic innovation domain where technological competitiveness, security and institutional resilience intersect.

The findings further demonstrate that DefenceTech innovation ecosystems are structured by interdependent organisational and institutional dynamics. Institutional barriers, including procurement timelines, export controls and security requirements, continue to influence ecosystem functioning, while startups emerge as central innovation actors requiring structured integration within defence institutions. At the same time, financing models increasingly reflect hybrid public–private investment approaches, and successful technology adoption depends on coordinated collaboration across armed forces, industry and innovation intermediaries. From a governance perspective, policymakers should prioritise rapid experimentation frameworks, investors should adapt to longer defence innovation cycles, and accelerators should align more closely with procurement structures.

Future research should focus on empirical evaluation of DefenceTech ecosystems, comparative analysis of NATO and EU innovation mechanisms, and the measurement of long-term innovation outcomes.

9. Conclusions

This article has addressed the question of how startups, financing mechanisms and acceleration instruments jointly shape technology adoption pathways within DefenceTech innovation ecosystems. The review demonstrates that startups have become central actors in defence innovation, particularly in software, AI and dual-use domains, yet remain structurally disadvantaged by procurement timelines, regulatory burdens and limited access to testing environments. Financing models are gradually adapting to these realities through hybrid public–private instruments, though capital allocation imbalances persist. Acceleration programmes such as NATO DIANA and EUDIS represent meaningful institutional responses, but their systemic impact remains nascent. The key theoretical contribution of this study lies in integrating these dimensions into a coherent analytical framework that treats the DefenceTech ecosystem as a co-evolutionary structure shaped by interdependent organisational, institutional and financial dynamics, an approach that has been underrepresented in the fragmented prior literature. These findings have direct implications for policymakers, investors and accelerators seeking to strengthen the absorptive capacity of defence innovation ecosystems.

10. Limitations

This study synthesises heterogeneous academic and policy sources rather than a single empirical dataset, which limits direct comparability between findings. The analysis focuses primarily on European and transatlantic DefenceTech ecosystems, reducing global generalisability. In addition, available data capture formal structures and policy instruments more effectively than informal or classified innovation activities.

References

Academic literature

Amir, D., & Rombach, C. (2025). *From startup to strategic asset: Success factors and barriers for startups in the Swedish defence ecosystem*. KTH Royal Institute of Technology.

Andersson, J. (2022). *Defence innovation ecosystems and startup integration in Sweden* (Master's thesis). Swedish Defence University.

Atkinson, R. (2025). Collaboration among NATO's defence innovators: Lessons from Poland. *Security and Defence Quarterly, 51*(3), 21–37. https://doi.org/10.35467/sdq/205139

Blagoeva, D., Pavel, C., Wittmer, D., Huisman, J., & Pasimeni, F. (2019). *Materials dependencies for dual-use technologies relevant to Europe's defence sector* (EUR 29850 EN). Publications Office of the European Union. https://doi.org/10.2760/570491

Carberry, S. (2023). Innovation acceleration. *National Defense, 108*(837), 31–32.

Caviggioli, F., De Marco, A., & Scellato, G. (2018). *Assessing the innovation capability of EU companies in developing dual use technologies* (EUR 29481 EN). Publications Office of the European Union.https://doi.org/10.2760/032120

Chen, X., Yang, Y., & Wei, J. (2024). How do new ventures thrive in ecosystem venturing: The impacts of alliance strategy and technology interdependence. *Journal of Management Studies*. Advance online publication.

Cheung, T. M. (2021). A conceptual framework of defence innovation. *Journal of Strategic Studies, 44*(6), 775–801. https://doi.org/10.1080/01402390.2021.1939689

Doumitt, A., Bycroft, B., Bissonnette, M., Vakki, O., Stern, I., Heinsheimer, T., & Bracey, M. (2025). Bridging the valley of death: A DoD/FFRDC partnership to accelerate low-TRL commercial space technology. *Proceedings of the Acquisition Research Symposium*. Naval Postgraduate School.

Fertasi, N. (2019). Why digital ecosystems of civil-military partnerships are a game changer for international security and defence. *Information & Security: An International Journal, 42*, 33–47.

French Ministry of Armed Forces. (2026). Agence de l'innovation de défense. https://www.defense.gouv.fr/aid

Graarud, S., & Kristensen, M. (2025). *Value creation in asymmetric innovation partnerships within the defence industry*. Linköping University.

Hajdú, F. (2025). A successful defence innovation ecosystem. *Honvédségi Szemle, 153*(Special Issue 1), 11–24. https://doi.org/10.35926/hdr.2025.1.2

Heidenkamp, H., Louth, J., & Taylor, T. (2011). The defence industrial ecosystem delivering security in an uncertain world. https://static.rusi.org/201106_whr_the_defence_industrial_ecosystem_0.pdf

Ilchenko, O., et al. (2021). The role of a defence industry in the system of national security: A case study. *Entrepreneurship and Sustainability Issues, 8*(3), 438–454. https://doi.org/10.9770/jesi.2021.8.3(28)

Knudsen, M., et al. (2025). The role of creativity and innovation management research in times of changing security and defence realities. *Creativity and Innovation Management, 35*(1). https://doi.org/10.1111/caim.70018

Kondrats, J., Pundure, J., & Jekabsone, I. (2025). Defence innovation ecosystems and rural economic development: Pathways to sustainable growth and military adaptation. *Research for Rural Development, 40*. https://doi.org/10.22616/RRD.31.2025.051

Liwång, H. (2022). Defense development: The role of co-creation in filling the gap between policy-makers and technology development. *Technology in Society, 68*, 101913. https://doi.org/10.1016/j.techsoc.2022.101913

McLeod, M. W. (2022). Venture capital and human capital patterns in dual-use hardware startups in the United States and United Kingdom. MIT Sloan School of Management.

Otaiku, A. (2021). Defence policy foresight | Military warfare ecosystem. *Global Journal of Arts, Humanities and Social Sciences, 9*(5), 34–63.

Schmid, J., & Wong, J. P. (2020). The role of new defense innovation intermediaries in the emerging defense innovation ecosystem. *Naval Postgraduate School. Acquisition Research Symposium*.

Schwarz, E. (2025). From blitzkrieg to blitzscaling: Assessing the impact of venture capital dynamics on military norms. *Finance and Society*, 1–24. https://doi.org/10.1017/fas.2024.18

Stasik, A. (2026). Beyond trade-offs: Dual-use social innovations for secure and sustainable futures. *Futures, 176*, 103752. https://doi.org/10.1016/j.futures.2025.103752

Wilson, J. (2024). Applying lessons from the commercial innovation system to the national security innovation base. *STEPS: Science, Technology, Engineering, and Policy Studies*, Issue 9, 26–37.

Ying, S. (2025). *Using predictive models to identify trends among successful dual-use startups*. Massachusetts Institute of Technology.

Grey literature

Center for Strategic and International Studies (CSIS). (2024). Space Threat Assessment 2024. Washington, D.C. https://aerospace.csis.org/wp-content/uploads/2024/04/240417_Swope_SpaceThreatAssessment_2024.pdf

European Commission. (2021). *EU funding programmes, Digital Europe Programme*. https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en

European Commission. (2023). *European Defence Industrial Strategy (EDIS)*. https://defence-industry-space.ec.europa.eu/eu-defence-industry/edis-our-common-defence-industrial-strategy_en

European Commission. (2024a). *Dual-use technologies in Europe: Strategic dependencies and recommendations*. http://rmis.jrc.ec.europa.eu/dualuse

European Commission. (2024b). *European Defence Industrial Strategy (EDIS) Joint Communication*. https://defence-industry-space.ec.europa.eu/edis-joint-communication_en

European Commission. (2024c). *Releasing the potential of dual-use research and innovation*. Publications Office of the European Union.

European Commission. (2024d). *White paper on dual-use R&D*. https://op.europa.eu/en/publication-detail/-/publication/1a54ebcd-bb98-11ee-b164-01aa75ed71a1/language-en

European Commission. (2025a). *EU defence industry transformation strategy: Releasing disruptive innovation for defence readiness*. https://defence-industry-space.ec.europa.eu/document/download/513de692-d08c-40cc-80c3-cb6611ace178_en

European Commission. (2025b). *European Commission takes steps to modernise European defence and improve military mobility*. https://commission.europa.eu/news-and-media/news/commission-takes-steps-modernise-european-defence-and-improve-military-mobility-2025-11-19_en

European Commission. (2025c). *Results of the European Defence Fund 2024 Calls for Proposals*. Brussels. https://defence-industry-space.ec.europa.eu/funding-opportunities-0/calls-proposals/result-edf-2024-calls-proposals_en

European Commission. (2025d). *White paper for European defence – Readiness 2030*. https://defence-industry-space.ec.europa.eu/eu-defence-industry/white-paper-european-defence-readiness-2030_en?utm_source=chatgpt.com

European Commission. (2026). *European Defence Fund (EDF)*. https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf[_en

European Court of Auditors. (2025). *Special report 12/2025: The EU's strategy for microchips*. Luxembourg. https://www.eca.europa.eu/ECAPublications/SR-2025-12/SR-2025-12_EN.pdf

European Defence Agency. (2023a). *Annual report 2023*. https://eda.europa.eu/publications-and-data/latest-publications/annual-report-2023

European Defence Agency. (2023b). *Coordinated Annual Review on Defence (CARD) – 2023 report*. Brussels. https://www.eeas.europa.eu/node/36453_en

European Innovation Council. (2026). *EIC Accelerator*. https://eic.ec.europa.eu

European Parliament. (2023). *Critical technologies for security and defence: State of play and future challenges*. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0131_EN.html

European Parliamentary Research Service. (2024a). *European Defence Industrial Strategy (EDIS)* [European Parliament Briefing]. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762402/EPRS_BRI(2024)762402_EN.pdf

European Parliamentary Research Service. (2024b). *European Defence Industrial Strategy (EDIS): Towards a more integrated and competitive European defence industry* [European Parliament Briefing]. European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762402/EPRS_BRI(2024)762402_EN.pdf

European Parliamentary Research Service. (2024c). *The geopolitics of technology: Charting the EU's path in a competitive world*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/762384/EPRS_BRI(2024)762384_EN.pdf

European Parliamentary Research Service. (2025). *Building a common market for European defence*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775924/EPRS_BRI%282025%29775924_EN.pdf

European Space Agency. (2023). Poland and ESA discuss plans for a new security-focused centre. https://www.esa.int/Space_in_Member_States/Poland/Polska_i_ESA_omawiaja_plany_utworzenia_nowego_centrum_bezpieczenstwa

European Space Agency. (2024). *Space Environment Report 2024*. Paris. https://www.esa.int/Space_Safety/Space_Debris/ESA_Space_Environment_Report_2024

European Space Agency. (2026). ESA Business Incubation Centres – Programme Overview. https://commercialisation.esa.int/esa-business-incubation-centres/

European Union. (2021). Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports of dual-use items. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0821

French Ministry of Armed Forces. (2026). Agence de l'innovation de défense. https://www.defense.gouv.fr/aid

In-Q-Tel. (2026). https://www.iqt.org

International Institute for Strategic Studies (IISS). (2024). *The Military Balance 2024*. London: IISS.

NATO Allied Command Transformation. (2025). Digital transformation and innovation activities. https://www.act.nato.int/activities/digital-transformation/

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2024). *CyCon 2024 Conference Proceedings*. Tallinn. https://ccdcoe.org/uploads/2024/05/CyCon_2024_book.pdf

NATO Innovation Fund. (2026). https://www.nif.fund

NATO Parliamentary Assembly. (2024). Critical dual-use technologies report. https://www.nato-pa.int/document/2024-dual-use-technologies-report-baldwin-051-esc

NATO Standardization Office. (2024). Allied joint doctrine for interoperability [STANAG documentation]. https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDB_V1_E_2525.pdf

NATO. (2012). Directive on the security of information. https://archives.nato.int/directive-on-the-security-of-information-3

NATO. (2022). NATO 2022 strategic concept. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

NATO. (2024). Interoperability of AI-enabled systems. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

NATO. (2025a). Emerging and disruptive technologies. https://www.nato.int/cps/en/natohq/topics_184303.htm

NATO. (2025b). Fast adoption action plan. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/summary-of-natos-fast-adoption-action-plan

NATO. (2025c). Science & technology trends 2025–2045. https://sto-trends.com/executive-summary/

NATO. (2026). DIANA. https://www.diana.nato.int/accelerator-programme.html

Naval Postgraduate School. (2020a). Defense innovation transition challenges. NPS Symposium Proceedings.

Naval Postgraduate School. (2020b). The effect of defense-sponsored innovation programs on market entry and competition. Monterey, CA: Naval Postgraduate School.

Organisation for Economic Co-operation and Development. (2024). How to best use STI policy experimentation to support transitions? https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/12/how-to-best-use-sti-policy-experimentation-to-support-transitions_99ddf48f/7b246309-en.pdf

Publications Office of the EU. (2024). White paper on options for enhancing support for research and development involving technologies with dual-use potential. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52024DC0027

RAND Corporation. (2024). The Chinese industrial base and military deployment of quantum technology (RAND Research Report). https://www.rand.org/pubs/testimonies/CTA3189-2.html

RAND Corporation. (2026). How artificial intelligence could reshape four essential competitions in future warfare (RRA4316-1). Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA4316-1.html

Stockholm International Peace Research Institute. (2024a). Top 100 arms-producing and military services companies (SIPRI fact sheet). https://www.sipri.org/publications/2025/sipri-fact-sheets/sipri-top-100-arms-producing-and-military-services-companies-2024

Stockholm International Peace Research Institute. (2024b). *SIPRI yearbook 2024*. Oxford University Press. https://www.sipri.org/yearbook/2024

Stockholm International Peace Research Institute. (2025). Yearbook 2025: Proliferation and use of missiles and armed uncrewed aerial vehicles. https://www.sipri.org/yearbook/2025/07

U.S. Department of Defense. (2022). Responsible artificial intelligence strategy and implementation pathway. Washington, D.C. https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.pdf

U.S. Department of Defense. (2023). Joint all-domain command and control (JADC2) strategy. Washington, D.C.

UK Cabinet Office. (2024). National security vetting. https://www.gov.uk/government/collections/national-security-vetting

UK Ministry of Defence. (2025). Defence industrial strategy: Making defence an engine for growth. https://assets.publishing.service.gov.uk/media/68bea3fc223d92d088f01d69/Defence_Industrial_Strategy_2025_-_Making_Defence_an_Engine_for_Growth.pdf

UK Ministry of Defence. (2026). Defence and Security Accelerator (DASA). https://www.gov.uk/government/organisations/defence-and-security-accelerator

United Nations Institute for Disarmament Research (UNIDIR). (2024). Quantum technology, peace and security. https://unidir.org/wp-content/uploads/2024/11/UNIDIR_quantum_technology.pdf