European Commission

Research and Innovation

Unlocking the potential of dual-use research and innovation

Independent Expert Report

Unlocking the potential of dual-use research and innovation

European Commission
Directorate-General for Research and Innovation
Directorate E — Prosperity
Maria Cristina Russo, Director
Unit E.1 — Industrial Research, Innovation and Investment Agendas
Contact Marco Grancagnolo
Doris Schröcker

Email Email maria-cristina.russo@ec.europa.eu
marco.grancagnolo@ec.europa.eu
doris.schroecker@ec.europa.eu
RTD-PUBLICATIONS@ec.europa.eu

European Commission
B-1049 Brussels

Manuscript completed in june 2025
First edition

PDF ISBN 978-92-68-25302-1 doi: 10.2777/5771805 KI-01-25-058-EN-N

Luxembourg: Publications Office of the European Union, 2025

EUROPEAN COMMISSION

Unlocking the potential of dual-use research and innovation

2025 Directorate-General for Research and Innovation

Contents

Authors

Unlocking the potential of dual-use research and innovation is a technical report published by the European Commission's Directorate-General for Research and Innovation, including as chapters the contributions of individual experts as follows (by alphabetical order of family name):

- Izabela Albrycht (AGH University of Krakow), for Chapter 1 on civil-defence synergies;
- Johan Evers (imec), for Chapter 2 on practical implementation of dual-use research and innovation, with focus on SMEs, start-ups and scale-ups;
- Karl Hallding (Vinnova), for Chapter 3 on policy strategies supporting dual-use research and innovation;
- Veronica Vella (University of Liège), for Chapter 2 on practical implementation of dual-use research and innovation, with focus on research performing organisations;
- André Xuereb (University of Malta), for Chapter 4 on funding programmes for dual-use research and innovation.

Foreword

The report *Unlocking the potential of dual-use research and innovation* by five experts comes at the right time in the current geopolitical context and for the preparation of the next generation of EU funding programmes. This work follows the *White Paper on options for enhancing support for research and development involving technologies with dual-use potential* and the related public consultation.

Recognising the importance of dual-use technologies as well as the challenges specifically related to their implementation in EU-funded projects, the experts with different backgrounds, both from the research and defence communities, offer insights with concrete examples and case studies on how dual-use research and innovation can work in practice.

The report offers an analysis on opportunities and challenges related to civil-defence synergies; uncovers practical implementation of dual-use research and innovation within the perspective of Research Performing Organisations and small and medium-sized enterprises, start-ups and scale-ups; and puts forward international examples and benchmarks on policy strategies and funding programmes supporting dual-use research and innovation. It also points to aspects for further analysis in this multi-faceted challenge.

Recent geopolitical and technological developments have impacted the world with potentially long-term consequences for European policies and society, influencing our economy, security and prosperity. It is against this background that the EU puts research and innovation at the heart of the economy, to foster competitiveness and technological sovereignty, as well as preparedness, security and defence. Advancing European leadership in dual-use technologies is an intrinsic part of the EU strategy to address critical dependencies, to shape international standards and to make the EU's role indispensable globally in value chains and in key industries. This is acknowledged in the White Paper for European Defence – Readiness 2030 and in the European Preparedness Union Strategy, as well as in the European Internal Security Strategy – ProtectEU.

The aim of this report is to contribute to a better understanding of dual-use research and innovation for an informed decision-making as the next generation of European programmes are under preparation. It is published at the same time as a policy brief of the Expert Group on the economic and societal impact of research and innovation (ESIR) on the implications of allowing dual-use research and innovation in the Framework Programme.

The key findings and conclusions of this work will certainly inspire further discussions across Europe and the Commission is looking forward to them.

Marc Lemaître

Director-General for Research and Innovation, European Commission

Executive summary and key findings

Civil-defence synergies

The rise of critical technologies, combined with growing geopolitical tensions, has triggered significant adjustments in Research and Innovation (R&I) models and priorities—both at national and EU levels. Civil-defence R&I synergies offer strategic opportunities to develop capabilities addressing both conventional (e.g., military conflicts, border tensions) and non-conventional threats (e.g., cyber-attacks, terrorism, illegal migration, climate change), while also advancing broader goals such as economic competitiveness and societal resilience.

However, a significant barrier to effective cross-fertilisation remains: companies, but more prominently SMEs and startups that initially focus on civilian applications and are open to entering the dual-use domain, often find themselves needing to scale down or reengineer their solutions late in the R&I process to meet defence-specific requirements. This adaptation is frequently costly, time-consuming, and strategically inefficient.

The potential for strengthening civil-defence synergies in the EU R&I landscape highlights the increasing recognition of the need to promote the diffusion of civilian-driven innovations to support future defence capabilities and reinforce the EU Defence Technological and Industrial Base. Supporting dual-use applications of critical technologies and fostering alignment between civil and defence research funding are central to this effort.

Key drivers of dual-use R&I are examined, including the strategic value of dual-use critical technologies, the civilian origin of many technologies essential for immediate defence needs, and the convergence of civil and defence challenges. The analysis of selected calls for proposals under Horizon Europe and Horizon 2020 assesses their relevance in a context of hybrid warfare and other emerging security threats. Drawing on stakeholder input gathered through surveys and interviews, major barriers to cross-fertilisation between civil and defence R&I are identified. The benefits and risks of dual-use innovation are outlined, offering insights for decision-makers on how to better integrate and support dual-use ecosystems across the EU's R&I framework.

The benefits of dual-use R&I are particularly evident at TRL 4–6 but also at lower TRLs, where technological synergies between civil and defence applications can be captured more effectively. That could be addressed by the establishment of a "dual-use-by-design model" within which the R&I process could integrate, if adequate and cost-effective, a simultaneous alignment with both civil and defence requirements or unified requirements, up to higher TRL levels, so only minimal modifications would be required to align a given technology with civil or defence standards when targeting the respective markets.

Facilitating access for newcomers to the defence sector through the dual-use pathway remains necessary. Nowadays, many successful entrants began with civilian-focused R&I activities, taking advantage of more accessible funding mechanisms. What could support a successful pathway for those companies choosing to develop dual-use solutions is positioning themselves within a broader security context (such as within the concept of systemic resilience, military mobility, critical infrastructure), which would help them gain access to wider market opportunities in both the civilian and defence sectors.

At the same time, dual-use development carries inherent risks. These include exposure of intellectual property to technology leakage, the need to ensure the confidentiality and integrity of sensitive research data, the challenge of creating secure project environments, and the requirement for personnel with both technical skills and appropriate security clearances.

To unlock the full potential of dual-use R&I, the opportunities that derive from early-stage integration of defence requirements should be captured, along with the creation of secure and trusted R&I environments, and through tailored guidance and incentives for dual-use actors, particularly SMEs and startups. Such measures are essential to ensure that critical technologies contribute meaningfully to Europe's strategic autonomy and its wider security and economic goals.

The key findings on synergies between civil and defence research and innovation (R&I) are highlighted as follows:

- The development of dual-use technologies addresses multipurpose objectives — namely enhancing defence and security, boosting competitiveness, and bolstering resilience.
- The persistent division between civilian and defence R&I is leading to a loss of competitive advantages in emerging technologies and in rapidly growing dual-use and defence markets.
- Many technologies developed within EU-funded civilian R&I projects exhibit dual-use characteristics that could contribute to specific defence and systemic resilience needs.
- The civil and defence sectors share similar threats, in particular in relation to critical infrastructures. Within the R&I process, civil-defence synergies can develop common capabilities to effectively respond to security and resilience challenges.
- Dual-use R&I can accelerate time-to-market by integrating both civil and defence requirements at early stage, thereby eliminating barriers to civil-defence technology transfer and facilitating uptake in the respective markets.
- At the same time, dual-use development carries inherent risks, which require the creation of secure and trusted R&I environment.

Practical implementation

The EU's effort to balance resilience, competitiveness, and security is closely linked to its evolving R&I policies, which increasingly highlight the role of dual-use research in strengthening both civilian and defence capabilities amid shifting geopolitical and strategic landscapes. As new funding opportunities arise for technologies with both civilian and defence applications, recipients will need to carefully assess whether their work falls under dual-use or military export control regulations.

Compliance with export controls is one of the most critical challenges in terms of practical implementation of dual-use R&I. Export control is required to regulate cross-border transfers of sensitive, strategic items with national security, terrorism or human rights considerations. In the EU, dual-use export control is an EU-level legally binding framework implemented by export control authorities in each EU Member State.

A comprehensive overview of the practical implementation of dual-use R&I focusing on compliance with export controls is presented. It highlights the complexities of defining dual-use technologies, which can serve both civilian and military purposes, and the impact of export controls on activities. The first part focuses on research-performing organisations (RPOs) whereas the second part addresses small and medium-sized enterprises, including start-ups, and relevant scale-ups.

Practical Implementation for Research Performing Organisations

The analysis of the lifecycle of EU-funded projects, from proposal to dissemination, and the comparison of different RPOs approach dual-use issues highlight significant variations in approaches in practice. Internal compliance programmes in RPOs are still emerging, and export controls are increasingly applied to research contexts, raising new questions and realities. Stakeholders recognise the significant value of engaging in dual-use research and would be further encouraged by a more favourable regulatory and operational environment. They have expressed a clear request for stronger engagement with export control authorities and increased support to navigate dual-use export control compliance challenges effectively. Both RPOs and export control authorities acknowledge shared challenges in compliance and enforcement and show a strong willingness to collaborate and improve the environment for effective implementation of EU-funded projects.

While dual-use items have not prevented participation in EU-funded projects, challenges such as administrative burdens and project implementation uncertainties persist. Specific challenges identified include managing consortium partnerships, uncertainties around open-access

publication, and licensing procedures that are subject to different national interpretations. Stakeholders propose measures such as stronger support from national and EU authorities, clearer guidance, dedicated points of contact, raising awareness among project participants, and ensuring a level playing field across EU countries.

Key findings to address the challenges of practical implementation of dealing with dual-use R&I faced by Research Performing Organisations (RPOs) are:

- There is potential for improvement concerning guidance on dual-use obligations, including open-access requirements. Training and national/EU-level campaigns can be introduced to support education and awareness, whereas dedicated resources and clear contact points can effectively boost RPOs compliance capacity.
- The introduction of a flagging mechanism for dual-use projects allows to identify sensitive research early and enable targeted EU support. In this regard, the strategic use of EU funding can raise awareness of dual-use research, promote secure collaboration and responsible innovation.
- Export control licensing can be adapted to better fit EU-funded projects, including exploring an EU-wide licensing system, while harmonisation across national licensing practices can be improved for a more consistent handling of requests.
- Policy efforts require consistency across export controls, research security, and economic security frameworks.

Practical Implementation for SMEs, Start-ups, and Scale-ups

The role of SMEs, including startups and relevant scale-ups, in dual-use R&I, the challenges they face in EU funding programmes, and the complexities concerning the implementation of export controls are analysed in depth. As SMEs, startups and scale-ups are often involved in prototyping, testing or demonstrating innovative products, they are not likely to meet the basic scientific research exemptions on export controls for dual-use items. These companies struggle with an overall overload of regulatory requirements and due diligence efforts and a lack of export control expertise.

Dedicated support mechanisms, including training, advisory services, and funding call triggers for export control compliance (and related expenses) are vital for those actors. Collaborating with export control authorities helps create compliance programmes and ensure regulations are followed. This reduces risks, ensures adherence, and supports the commercialisation of technologies aligned with EU security objectives.

Recurring misunderstandings concerning the impact of export controls are highlighted and three main challenges in implementing export controls are identified: classifying items, using Technology Readiness Levels as export control triggers, and managing item transfers between EU and associated country partners. This part concludes with suggestions for additional export control triggers and alerts in the funding programme guidance notes.

The lack of indicators for targeted R&I calls with a higher likelihood of involving dual-use items or application areas, the unawareness among applicants/beneficiaries of export control rules during different stages, the limited information exchange between funding and export control authorities on R&I projects involving dual-use items, and the minimal screening of project deliverables for dual-use items, all contribute to a blind spot concerning export controls for all stakeholders today.

Many SMEs can significantly benefit from R&I funding calls that indicate the need or requirement for export control due diligence, from further guidance on how to identify (classify) a dual-use or military item, from further simplification and harmonisation of export control rules and implementation across the EU. SMEs, including startups and relevant scale-ups, and other beneficiaries active in dual-use R&I benefit from a whole-of-government approach fostering innovation, balancing economic interests with national security and non-proliferation objectives, and enhancing due diligence capabilities.

Key findings to address the challenges of practical implementation of dealing with dual-use R&I faced by SMEs, including start-ups and scale-ups are:

- It would be beneficial for SMEs involved in dual-use goods, software, and technology to receive tailored export control due diligence guidance.
- For projects focused on defence or security applications or producing results of relevance for defence or security applications, it is crucial to implement consistent dual-use or military export control checks.
- Best practices from granted projects that have effectively managed export controls can be gathered and used as examples for future applicants.
- Programme managers can be trained to assist SMEs, manage dual-use projects, and liaise with export control authorities.

International benchmarks

Policy strategies supporting dual-use research and innovation

Dual-use R&I has emerged as a strategic priority in response to evolving geopolitical dynamics and transformative technological developments. Over the past decade, many countries have gradually shifted from fragmented or defence-centric models to more integrated strategies that strengthen the dual-use potential of national R&I systems. This evolution has been shaped by the growing influence of commercially driven innovation in areas such as AI, biotechnology, and semiconductors, combined with heightened concerns over national security, economic resilience, and technological sovereignty.

National approaches to dual-use R&I are compared across three strategic dimensions: anticipatory technology foresight, civil–military innovation integration, and research security and responsible internationalisation. The analysis draws on a structured review of policy strategies, expert reports, and institutional frameworks from a diverse set of countries, including the United States, China, Israel, Japan, the United Kingdom, and a range of EU Member States.

Recurring strategic approaches and institutional models that support the alignment of innovation and security objectives are not only visible in formal policy frameworks but also in dynamic innovation ecosystems – such as Silicon Valley, Israel's defence-linked startup sector, and other hubs where trust-based, dual-use collaboration has long underpinned advanced innovation and global technological leadership. In several of these ecosystems, structured mechanisms for spinning off defence-funded technologies into civilian markets – such as NASA's Technology Transfer Program or the UK's Ploughshare Innovations – further illustrate how defence-driven R&I can generate broader societal and economic value.

Key findings that reflect how countries are responding to common challenges in this domain are as follows:

- Shared responsibility is a key enabler of dual-use R&I: trust-based collaboration between government, research institutions, investors, and defence actors – as seen in ecosystems like Silicon Valley and Israel's startup sector – supports both risk awareness and opportunity-driven innovation.
- Trusted networks are shaping the future landscape of dual-use international collaboration: initiatives such as NATO DIANA and bilateral alliances among like-minded states provide structured frameworks for secure cooperation in dual-use technologies.
- Strategic foresight and innovation pipelines are increasingly integrated: governments use roadmaps, scanning platforms, accelerators, and public-private schemes to guide investments in dual-use technologies. Notable examples include INNOFENSE (Israel), DASA (UK), and the Defense Innovation Unit (DIU) (US).
- Balancing openness with security is a growing priority: countries such as Finland and Sweden are introducing due diligence frameworks procedures and institutional

guidance to enable responsible internationalisation while protecting sensitive knowledge.
- Talent and workforce development are gaining strategic importance: mobility schemes, fellowships, and startup visas – such as those in Germany and the UK – are being used to attract critical skills and strengthen dual-use innovation capacity.

Funding programmes for dual-use R&I – an international comparison

The comparative benchmarking analysis of dual-use R&I funding systems in the USA, the People's Republic of China (PRC), Japan, the Republic of Korea (ROK), the UK, Finland, Israel, and NATO shows the different policy backgrounds underpinning each system; the specific features of its funding instruments for dual-use R&I; and the international context relevant to it, using publicly available information.

In addition to documenting the structural features of these funding systems, notable examples of good practice are highlighted: DARPA in the US as the gold standard for funding dual-use R&I, the identification by the PRC government of quantum communications as a national priority, mechanisms for formal consultation with dual-use startups in Japan, inter-ministerial coordination in the ROK to promote the visibility of civilian solutions for defence use, mechanisms to facilitate uptake of new dual-use technologies in Israel, the export market of dual-use technologies as an economic driver in Finland, and how the UK system both assists with issues surrounding foreign researchers working on dual-use R&I and facilitates the transfer of R&I between the civilian and defence markets.

Despite differences in governance models and strategic priorities, common patterns emerge across these systems. A set of themes are identified, which could serve as a useful reference in the design of future dual-use R&I policies and funding programmes, particularly in the European context.

Across the international landscape of funding programmes for dual-use R&I, key findings are:

- Such programmes are compatible with defensive-only or pacifist stances (Japan) and promote both economic development and national security (Republic of Korea).
- To support a range of TRLs, funding systems can mix bottom-up strategies with top-down support for specific technologies (China) or challenges (NATO DIANA).
- Simplified landscapes for dual-use funding programmes may result from splitting funding programmes according to TRLs (Finland, MEIMAD [Israel], NATO).
- The participation of foreign entities or researchers is limited by safeguards (US, UK) and prioritises the bringing of knowledge into a country (Israel).
- Support for SMEs, such as fast tracks to procurement (DIU and DARPA [US]) and simplified regulations (Israel), may facilitate the adoption of new technologies.

1. Civil-defence synergies

1.1. Introduction

A technological revolution is ongoing worldwide. An exponential growth rate of research and innovation (R&I) in the civil sector offers exceptional opportunities for technologies with dual-use potential. Raising conventional (military conflicts, border tensions, airspace violations) and non-conventional (e.g. cyber-attacks, illegal migration, terrorism, or climate change) security threats increasingly require a technological answer.

This chapter provides evidence on potential civil-defence synergies to support informed political and policymaking in the EU. It examines, in its first section, the methodology used, then it identifies main barriers to dual-use R&I, and in its third section analyses the key drivers, benefits and risks of civil-defence synergies.

The selected methodology combines a literature review of recent reports and official EU and NATO documents with an analysis of a case study on Ukraine's R&I ecosystem. Additionally, an in-depth qualitative assessment was conducted based on a Survey distributed[1] by the author to selected innovators – chosen for their relevance to dual-use technologies and solutions, among coordinators in Horizon Europe and Horizon 2020 projects, industry leaders, SMEs, and startups - particularly those from NATO Defence Innovation Accelerator for the North Atlantic (DIANA) cohorts, as they have recognised dual-use technology. The Survey was addressed to innovators working on technological areas which covers the most prominent critical technologies, such as: artificial intelligence (AI), autonomous systems, quantum technologies, biotechnology, hypersonic systems, space technologies, advanced materials and manufacturing, energy and propulsion, next-generation communications networks, cyber and information technologies (IT). Participant observation, understood as an immersive research method in which the observer actively engages in the environment while systematically collecting data, was also a key element of the adopted methodology which contributed with R&I community insights.

The scope and timeframe of the study has imposed certain limitations on the representativeness and quantitative significance of the Survey, which were to a certain extent compensated through 15 interviews with stakeholders from the Survey sample. It was also not possible to cover specific topical risks or conditions, such as interoperability of standards for civil and defence sectors, regulatory barriers or ethical considerations. However, the findings from the Survey and follow-up interviews provide a valuable sample of expert opinions and qualitative insights that highlight the key challenges and opportunities within the European dual-use technologies ecosystem in the making, which were also identified through desk research and participant observation processes.

[1] The Survey addressed to R&I project coordinators, companies and experts was distributed in February 2025 among 80 respondents. The time frame for response took place between 15 and 28 February 2025. The response rate was 40% (32 respondents), distributed as follows: 18 respondents from the private sector, 8 from academic community and 6 independent experts.

1.2. Main drivers for dual-use R&I

1.2.1. Growing importance of critical technologies of dual-use nature for EU's strategic goals

Advanced technologies have become powerful instruments of both soft and hard power, supporting geopolitical rivalry and geoeconomic competition between states. The growing interdependence between geopolitics and technology, often referred to as a 'geo-technological race'[2], is characterised by the disruptive role of innovation occurring at the intersection of various critical technologies of a dual-use nature. Critical technologies are fostering innovation, generating economic value, and reshaping all types of industries including defence. They are also helping to formulate an answer to crisis of globalisation, security threats or global challenges, such as climate change. Therefore, the development of critical technologies addresses multipurpose objectives, namely enhancing defence and security, boosting competitiveness[3] and bolstering resilience. This should be recognised as the primary driver for dual-use R&I.

These three crucial goals will be particularly important in driving the need to stimulate the cross-fertilisation of civil-defence R&I. Support to dual-use technologies is reflected in the Commission President's Political Guidelines[4], while their role is outlined in the Commission's *White Paper on options for enhancing support for research and development involving technologies with dual-use potential*, which emphasizes the need to address "the gap between exclusively civil and exclusively defence R&D activities, in particular on critical and emerging technologies"[5]. The Commission 2025 Work Programme is also addressing the need to boost EU competitiveness, security and resilience[6].

Close attention to enhancing defence and security is justified in response to Russia's war of aggression against Ukraine[7]. This has already accelerated the adjustment of EU's strategic goals linking defence and security priorities with resilience and technological sovereignty[8]. The need to increase EU security, including cybersecurity, occurs also to be a main strategic goal for Poland's EU Council Presidency, which started on 1 January 2025 with the "Security, Europe!" and it is further politically enhancing the need to strengthen synergy of civilian and defence R&I[9]. In fact, there is a broad understanding and an evolving policy support to the need of promoting the diffusion

---

[2] The term "geotechnology" as the influence of technology on power projection and on building geopolitical and geoeconomic advantages by states was introduced by Stephen Robert Nagy. Cf. Nagy (2018), 'Geotechnology meets geopolitics: US-China AI Rivalry and Implication for Trade and Security'. See also, Rekowski et al. (2020), 'Geopolitics of Emerging and Disruptive Technologies', p. 64.

[3] See also the Industrial R&D Investment Scoreboard, the SRIP reports, the Draghi report or the report EU Innovation Policy - How to Escape the Middle Technology Trap | IEP@BU.

[4] '*We will look at all of our policies through a security lens (…). Firstly, the Commission will prioritise advancing Europe's economic security and economic statecraft. This means boosting our competitiveness at home and investing in research capacity for strategic and dual-use technologies that are essential for our economy and security*', Von der Leyen (2024), 'Political Guidelines for the next European Commission 2024-2029'.

[5] European Commission (2024), *White Paper on options for enhancing support for research and development involving technologies with dual-use potential*.

[6] European Commission (2025), *2025 Commission work programme*.

[7] '*In view of the challenges we face and in order to better protect our citizens, while acknowledging the specific character of the security and defence policy of certain Member States, we must resolutely invest more and better in defence capabilities and innovative technologies*', Council of the European Union (2022), *Informal meeting of the Heads of State or Government: Versailles Declaration*.

[8] European Commission (2022), *A Strategic Compass for Security and Defence*.

[9] '*We understand that shared security is not only about enhancing Europe's defensive capabilities but also about ensuring competitiveness, energy independence, and food security. Together, we are building a unified foundation for economic security – Europe's competitiveness in the global race for innovation and technological development*', Tusk (2025), 'Security, Europe! [Speech]'.

of civilian innovative technologies and solutions to enhance the development of future defence and military capabilities and strengthen the EU Defence Technological and Industrial Base (EDTIB)[10][11].

Fostering R&I in cutting-edge dual-use critical technologies also makes economic sense. Boosting EU competitiveness, as recommended by the Draghi report[12] and the Heitor report[13], should be achieved through i.e. highly likely increase in strategic R&D investments to close the EU's innovation gap, creating Advanced Research Projects Agency (ARPA)-style programmes for high-risk projects, and reallocating funds to boost startups and scale-ups via simplified, market-driven R&I ecosystems, prioritising disruptive technologies (e.g., AI, quantum) and dual-use applications (civil-defence synergies) and aligning dual-use tech development with civil-defence industrial needs. Harnessing these technologies and positioning them at the forefront of economic development and defence preparedness will strengthen EU's strategic autonomy and its economic security.

Finally, bolstering resilience is comprehensively covered in the Niinistö report[14], building on the need to tackle converging threats faced by EU countries, with reference to crisis-resilient infrastructure, resilient economy, climate-resilience, resilience of space systems, resilience of its industrial and supply chain, resilience of water supply and wastewater entities, societal resilience, cyber-resilience, building on the need to tackle converging threats faced by EU countries. The Preparedness Union Strategy explicitly refers to the need to promote dual-use by design, including for technologies that support both civilian and military needs[15]. Since the Niinistö report puts a strong emphasis on mutual resilience built together with partners, cooperation with NATO will be important. In times of rapid technological transformation, dual-use technologies can strengthen a systemic resilience, as further described in this chapter.

The interplay between these three crucial goals is expected to significantly drive investment in dual-use R&I in the EU, while building on broader converging trends, such as rising defence spending in EU Member States, the globally growing tech market for dual-use technologies, coupled with increasing Venture Capital (VC) investments[16][17], financial backing from institutions like the European Investment Bank (EIB) and the European Investment Fund (EIF), as well as supportive policy strategies for dual-use technologies (see chapter 3). It is expected that these investments will have also a significant positive impact on the EU economy[18].

1.2.2. The civilian origins of technologies critical for immediate defence needs

Another main driver of dual-use R&I and the need to develop synergies between the civilian and defence sectors is the fact that the majority of critical technologies and solutions, while having civilian origins, have wide applicability for defence purposes. They can help building new capabilities for the defence sector and addressing the innovation and defence capability gaps in the seven priority areas which are critical to build a robust European defence, presented in the

[10] As highlighted in the European Commission's 'Roadmap on critical technologies for security and defence' (2022), many breakthrough innovations initially developed for civilian purposes later become indispensable for defence and security.
[11] European Commission (2025), *Joint White Paper for European Defence Readiness 2030*.
[12] Draghi (2024), *The future of European competitiveness: A competitiveness strategy for Europe*.
[13] European Commission (2024), *Align, Act, Accelerate: Research, Technology and Innovation to boost European Competitiveness.*
[14] Niinistö (2024), *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*.
[15] European Commission (2025), *Joint Communication on the European Preparedness Union Strategy*.
[16] In 2023, VC investment in defence technology surged to USD 35.8 billion, a dramatic rise from USD 1.9 billion just a decade earlier, cf. Bower (2024), 'Venture Capital Investment in US National Security'.
[17] VC investments in defence-related companies jumping by 33 percent year-over-year to USD 31 billion in 2024, cf. Swartz, and Brukardt (2025), 'Creating a modernized defence technology frontier'.
[18] See for example Sezal, and Giumelli (2022), 'Technology Transfer and Defence Sector Dynamics: the case of the Netherlands'; and Moretti, Steinwender, and Van Reenen (2019), 'The intellectual spoils of war? Defence R&D, productivity and international spillovers'.

Joint White Paper for European Defence Readiness 2030[19]. As the case study on Ukraine demonstrates, the deployment of civilian technologies for defence purposes offered clear short-term strategic advantages.

Box 1: Case study: Dual-use R&I in Ukraine

The war in Ukraine may go down in history as the most technologically advanced conflict that manifests civil and defence applications of critical technologies. Every day, it provides evidence of changes in modern warfare, spanning over all domains of operations, integrating cyber-offensive and cyber-defensive actions, space capabilities, AI, and many more dual-use critical technologies. For three years now, the Ukrainian army, government, and society have collectively withstood Russian military attacks despite Russia's significant numerical superiority[20]. Commercial off-the-shelf (COTS) solutions played a crucial role, followed by the agile and rapid development and adoption of dual-use technological solutions[21]. This conflict has illustrated that technologies originally designed for civilian purposes can be repurposed for defence applications and offer significant military advantages, while also reducing casualties. Altogether, modern warfare increasingly depends on swift deployment of civilian technology. This trend is likely to further shape future conflicts and requires adaptation strategies and relevant innovation ecosystems leveraged by governments. The Ukrainian example demonstrates that technology originally developed for commercial use can be successfully applied to warfare challenges. With the ability to rapidly adapt to these new battlefield realities, technology has become Ukraine's 'secret weapon'. That is why Ukraine's experience is closely observed and analysed and serves as a strong signal to the EU leaders on what would be needed in case of a wartime emergency requiring fast and effective technological and organisational adaptation of the R&I processes and technology transfer.

Consequently, it also reveals profound implications for EU R&I ecosystems. It illustrates the practical need of establishing the EU-wide dual-use framework, delivering on innovative technologies that can be used for both civilian and defence purposes in real-world scenarios. This situation exemplifies why EU's recent policy initiatives emphasise the need for strategic investment in critical emerging technologies with dual-use potential, acknowledging that many cutting-edge research fields simultaneously serve civil innovation goals while carrying out security and defence implications. The conflict thus provides a tangible case study reinforcing the direction towards responsible development of dual-use technologies within the EU R&I framework. These changes will likely trigger EU-wide reflection that fast development, deployment and integration of new defence capabilities into armed forces, government and security organisations is now a critical need.

Source: The author.

Development of critical technologies has been in many respects dominated by civilian-oriented R&I activities, which for many years have developed more dynamically than defence-oriented ones. As a result of the "peace dividend", the European defence industry has suffered from low defence spending and lack of focus on technological development. In Europe, funding for defence R&D was EUR 10.7 billion in 2022, amounting to just 4.5% of total defence spending, as compared to 16% in the US[22]. Most EU Ministries of Defence '*currently lack the organisation, structures, focus, ambition, and talent to effectively innovate at scale*'[23]. From this perspective, seeking dual-use applications of civil critical technologies and enhancing greater synergies between civilian-

[19] At least 4 out of 7 priority capability areas can benefit from dual-use applications of civilian technologies, that is Drones and counter-drone systems: unmanned systems, including aerial, ground, surface and underwater vehicles that can be controlled remotely or operate autonomously using advanced software and sensors and enhance the capabilities that these technologies enable (e.g. situation awareness, surveillance, …); Military Mobility: an EU-wide network of land corridors, airports, seaports and support elements and services, that facilitate the seamless and fast transport of troops and military equipment across the EU and partner countries; AI, Quantum, Cyber & Electronic Warfare: defence applications using military AI and quantum computing; EU-wide advanced electronic systems; Strategic enablers and critical infrastructure protection: including but not limited to Strategic Airlift and Air-to-Air refueling aircraft, intelligence and surveillance, maritime domain awareness, use and protection of space and other secure communications assets and military fuel infrastructure. Cf. European Commission (2025), *Joint White Paper for European Defence Readiness 2030*.

[20] Ukraine spent USD 4.7 billion in 2021, just over a tenth of nuclear-armed Russia's USD 45.8 billion, according to the International Institute for Strategic Studies' *The Military Balance 2021*.

[21] The remarkable examples include commercial drones for reconnaissance and artillery spotting; commercial satellite internet terminals like Starlink, supplying high-resolution imagery, timely and accurate information and better operational planning by ICEYE. See also Bondar (2025), 'How Ukraine Rebuilt Its Military Acquisition System Around Commercial Technology', and ICEYE (2024), 'ICEYE and the Ministry of Defense of Ukraine sign a Memorandum of Cooperation'.

[22] Draghi (2024), *The future of European competitiveness: A competitiveness strategy for Europe*.

[23] Schlueter et al. (2022), 'Closing the Defense Innovation Readiness Gap'.

oriented and defence-oriented research funds, programmes and priorities (through EDF and Horizon Europe) can provide quick benefits supporting defence and resilience.

Reflecting on the Niinistö report's call for the EU to better leverage its spending by enhancing the dual-use potential of investments and unlocking dual-use research possibilities, the author decided to explore on a theoretical level whether technologies supported by civilian research and innovation programmes such as Horizon Europe and Horizon 2020 could also contribute to defence-related needs. It is important to note that the author does not claim that these technologies or project outcomes are directly applicable to defence nor that the projects concerned did not focus exclusively on civil applications. Instead, the focus is on identifying their potential to form the basis for dual-use solutions, i.e. technologies that, with adaptation or further development, could meet both civilian and military requirements. This theoretical exploration also touches on another key point raised in the Niinistö report: the need for a cultural shift within the EU. The Niinistö report emphasizes moving away from a strict separation between civilian innovation and defence needs, instead fostering a mindset where civil-military synergies and dual-use opportunities are integrated from the outset. According to the Niinistö report, maintaining this artificial divide is no longer financially or strategically sustainable[24].

Table 1: Examples of Horizon Europe / Horizon 2020 projects that deal with technologies that are also identified in NATO DIANA call for proposals

Technology	Examples of projects with given technology as main (M) or supporting (S)	Comments
Cyber-physical security	CIPSEC (M), DEFENDER (M), SAURON (M)	Comprehensive protection of critical systems connecting the physical and digital worlds (including ports, power grids, industry).
Quantum/post-Quantum cryptography	EPOQUE (M)	Projects focusing strictly on quantum and post-quantum cryptography.
Artificial Intelligence (AI), Machine Learning (ML)	DeeViSe (M), Drones4Safety (M), AGILEFLIGHT (M), MARISA (M), ARESIBO (M)	Mostly used for image analysis, drone autonomy, sensor data fusion, event prediction, etc. In a great number of projects, it plays a supporting role.
Materials science (i.e. new materials)	GRAPH-IC (M), HEATPACK (M)	Development of new materials (graphene photodetectors, thermal materials for space applications).
Biometrics	D4FLY (M)	E.g., for the purpose of identity verification using biometrics (iris, face) and document forgery detection.
Drone surveillance	IDEAL DRONE (M), Drones4Safety (M), RESPONDRONE (M), ROBORDER (M)	Projects developing drone fleets for rescue, infrastructure inspection and border protection.
CBRN detection and defence	TOXI-triage (M), eNOTICE (M), TERRIFFIC (M), EuRAdion (M)	Projects focused on detection and response to chemical, biological and radiological threats, including training of services and development of rapid triage tools.
Autonomy (unmanned vehicles, drones, robots)	ROBORDER (M), AGILEFLIGHT (M), ENDURUNS (M), RESPONDRONE (M), ARESIBO (M)	It most often refers to autonomous drones (air, sea, underwater) equipped with AI.

Source: Analysis performed by the author, supported by Artificial Intelligence; ChatGPT. chat.openai.com/chat. 23 Feb 2025. Model: o1 pro

[24] Niinistö, S. (2024), *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*.

As a basis to perform the assessment, the NATO Defence Innovation Accelerator for North Atlantic (DIANA)[25] challenges were used as reference framework. Based on descriptions provided in the EU Funding and Tenders Portal, many technologies developed in these civilian projects exhibit characteristics that could contribute to those specific defence needs. Among the most common technology areas, Artificial Intelligence (AI) and Machine Learning (ML) are the most frequently encountered themes, both as a primary technology and as a supporting technology. Leading themes are also cyber-physical security, Chemical, biological, radiological and nuclear (CBRN), advanced sensing/drones, and novel high-tech materials.

This analysis provides evidence of the dual-use nature of critical technologies developed within EU civilian-oriented programmes, compared to the following NATO's DIANA dual-use challenges:

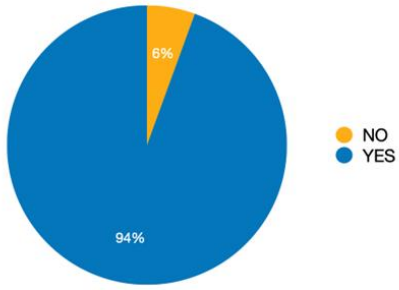
- *Energy & Power Challenge* focusing on "enhancing resilience in energy and power across various contexts, including generation, storage, distribution, recovery, harvesting, and access across land, sea, air, and space"[26] such as projects, oriented on protection of critical energy infrastructures, advanced cybersecurity, monitoring and protection solutions specifically tailored to energy infrastructure or innovative power generation solutions (examples: DEFENDER, SPEAR, SDN-microSENSE, SecureGas, ENDURUNS);
- *Data and Information Security Challenge* aiming at ensuring the secure and reliable generation, exchange, processing, and validation of data and information, particularly in multi-domain environments that encompass diverse devices, communication networks, operational contexts, and applications across both civilian and military sectors[27], such as projects focused on practical post-quantum cryptographic solutions, coordination of various threat-detection methods and incident-response, trust and security solutions for complex IoT ecosystems or exploring cyberdefensive measures (examples: EPOQUE, CIPSEC, ARCADIAN-IoT, MALFOY);
- *Sensing & Surveillance Challenge* aiming at enhancing operational awareness, improving threat detection, and ensuring effective monitoring, forecasting, early warning, situational awareness, post-action assessment, decision-making, and behavioural analysis with the use of systematic observation of physical domains, places, or things using a variety of sensors, including optical, radio, acoustic, and magnetic[28], with projects proposing a new approach to maritime or border surveillance, integrating information from diverse sensors and systems, and introducing advanced acoustic, thermal, optical, infrared, radar sensing, combined with AI-driven methods (examples: RANGER, MARISA, ROBOARDER, FOLDOUT, COMPASS2020);
- *Human Health & Performance Challenge* focusing on optimising human health and performance, which connect physical and psychological well-being, resilience, and recovery. This requires innovative dual-use solutions that enhance real-time monitoring and predictive analysis in extreme and complex environments, such as military operations, disaster response, sports and athletics, and space exploration[29], with projects aimed at integrating sensor-driven robotics, drones, advanced detection tools, interconnected wearable sensors and AI-driven tools, sensor-based monitoring solutions (examples: TOXI-triage, INGENIOUS, ASSISTANCE, CURSOR, RESPONDRONE);
- *Critical Infrastructure & Logistics Challenge* focusing on strengthening the resilience of critical infrastructure and supply chains, which are increasingly interconnected and vulnerable to disruptions[30], with projects combining advanced detection, modelling, and

[25] NATO, DIANA - Homepage, available at: https://www.diana.nato.int/.
[26] NATO, 2024 DIANA Challenge Programme Call For Proposals, available at: https://www.diana.nato.int/resources/site1/general/2024_challenge_programme_web.pdf.
[27] *Ibidem.*
[28] *Ibidem.*
[29] *Ibidem.*
[30] *Ibidem.*

response mechanisms for cyber-physical threats, including for space-based infrastructure (examples: ATENA**,** InfraStress, 7SHIELD, Drones4Safety, C-BORD).

Additionally, the survey among companies working within critical technologies fields as well as an overview of the technologies introduced to DIANA by civilian startups were conducted to support above thesis with even more evidence.

Figure 1: Can your solution/technology have dual-use potential?



Source: Survey by the author, February 2025.

Note: * *Dual-use potential means it can be relevant to both civil and defence domains, including applications that support the state's systemic resilience (such as continuity of government and critical government services—for instance, resilient energy supplies; resilient food and water resources against disruption or sabotage; the ability to manage mass casualties and disruptive health crises; resilient civil communications systems; and resilient transport systems).*

***The survey sample included 80 respondents, out of which 24 (30%) replied. An explanation of the survey sample is provided in the methodological section of this chapter.*

Moreover, the range of critical technologies introduced to DIANA by civilian startups holds the dual-use potential. In the field of Human Health & Performance Monitoring, companies such as Cogitat, Flosonics Medical, RealNose Inc., Qidni Labs, and Interact Technologies have developed technologies for non-invasive health tracking, brain-computer interfaces, and exoskeletons for rehabilitation and performance enhancement, which can be used for defence applications. Similarly, advancements in Biothreat Detection & Sterilisation are evident in solutions like airborne pathogen elimination and biomarker analysis platforms for early health risk detection, introduced by Gamma Pulse and 52North. The sector of Advanced Biotech & Pharmaceutical Production has also seen breakthroughs, with innovations in mRNA production and AI-driven drug discovery from companies such as Sensible Biotechnologies and QurieGen. In the area of Next-Gen Energy & Power Systems, startups like APR Technologies AB, Atomiver, Hydrogen Refinery, and Tactical Edge Systems have contributed with solutions for efficient cooling, supercapacitors, synthetic fuel production, and mobile energy generation. The critical domain of Data Security & Quantum Communications is also experiencing transformation, with BioSistemika, CUbIQ Technologies, ResQuant, and Factiverse developing DNA-based data storage, quantum-secure encryption, and AI-powered fact-checking. Finally, in Surveillance & Detection Technologies**,** AI GPR and STARNAV have introduced advanced sensors for underground object detection and GPS-independent navigation. These examples demonstrate how civilian startups are actively shaping dual-use innovations, bridging technological advancements between commercial and defence applications.

1.2.3. The convergence of civil and defence challenges and needs

For the last few years, we have been observing the high degree of alignment in capability demands of civil and defence sector. This is mainly due to the fact that critical infrastructures are often shared between civil and defence sectors to serve their respective needs. That is why the need to enhance resilience of critical infrastructures is a driver of civil-defence synergies, including through dual-use R&I, which could lead to developing technological solutions to protect it. The rising importance of

critical infrastructures is a result of the emergence of threats that target these crucial facilities in hybrid warfare operations, as well as the changing nature of modern conflicts which is heavily dependent on civil infrastructures such as transport, energy or communication systems.

Hybrid warfare is characterised by various actions and campaigns of destabilisation that include cyberattacks and incidents of sabotage, such as damaging critical infrastructures, jamming communication systems, derailing trains, committing acts of arsons[31]. Typically, they are classified below the threshold of war and, therefore, fall mainly under the responsibility of the civil security sector - police forces, internal security agencies, border authorities, custom agencies, as well as private security services. However, there are also concerns and challenges for defence stakeholders as the modern conflict very much depends on civilian critical infrastructures, including digital infrastructures: '*around 90 per cent of military transport for large military operations is provided by civilian assets (…); over 70 per cent of satellite communications used for defence purposes are provided by the commercial sector; approximately 95 per cent of transatlantic internet traffic, including military communications, is carried by undersea fibre-optic cable networks, most of which are owned and operated by private sector entities; on average, around 75 per cent of host nation support to NATO operations is sourced from local commercial infrastructure and services*'[32].

In fact, "a failure in essential systems, such as power grids or water supplies, can create cascading effects that compromise supply chain operations, potentially exposing them to cyber-attacks that disrupt manufacturing, transportation, and logistics"[33]. This reality was reflected in the NATO concepts of civil preparedness, and state's systemic resilience[34], the DIANA challenges presented above (Critical Infrastructure & Logistics Challenge, Energy & Power Challenge*).* On the EU side, it was widely reflected in the *Joint White Paper for European Defence Readiness 2030*, which states that "for their movements, the armed forces need access to critical transport infrastructure that is fit for a dual-use purpose", as well as that the dual-use infrastructures is essential for "space-based communications, navigation, and observation"[35].

For these reasons, the need to enhance security and resilience of critical infrastructures should be considered as a driver of dual-use R&I. The analysis of calls for proposals in both Horizon Europe and its predecessor, Horizon 2020, also clearly illustrates the aim to address emerging security challenges, including hybrid warfare threats. Many Horizon Europe calls under Cluster 3 (*Civil Security for Society*) concentrate on increasing the resilience of critical infrastructures (e.g. energy, water and food supply, health). The expected outcomes aim to support operators' resilience to natural and human-made threats and hazards, as well as to improve monitoring, risk assessment, forecast, mitigation and modelling techniques (for example Resilient Infrastructure's call HORIZON-CL3-2024-INFRA-01-01[36]); contributing to secure services, processes and products, as well as to robust digital infrastructures capable to resist and counter cyber-attacks and hybrid threats through advanced cybersecurity solutions (Increased Cybersecurity's call HORIZON-CL3-2024-CS-01[37]); as well as enhancing security against emerging threats, for example with Post Quantum Cryptography (HORIZON-CL3-2024-CS-01-02[38]).

[31] Appathurai (2025), 'European Parliament Committee on Security and Defence, In association with the Delegation for relations with the NATO Parliamentary Assembly'.
[32] Niinistö (2024), *Safer Together – Strengthening Europe's civilian and military preparedness and readiness*.
[33] NATO, 2024 DIANA Challenge Programme Call for Proposals.
[34] Cf. NATO (2024), 'Resilience, civil preparedness and Article 3'.
[35] European Commission (2025), *Joint White Paper for European Defence Readiness 2030*.
[36] Available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/HORIZON-CL3-2024-INFRA-01-01?order=DESC&pageNumber=1&pageSize=50&sortBy=startDate&keywords=HORIZON-CL3-2024-INFRA-01-01&isExactMatch=true&status=31094501,31094502,31094503.
[37] Available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2024-cs-01-01.
[38] Available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2024-cs-01-02.

Table 2: EU funded projects relevance to hybrid warfare threats[39]

Call ID	Focus	Relevance to hybrid warfare threats
HORIZON-CL3-2024-CS-01-01	Security in software/hardware development	Mitigates vulnerabilities exploited in cyber-enabled hybrid attacks.
HORIZON-CL3-2024-CS-01-02	Transition to post-quantum cryptography	Protects critical communications/data from advanced cyber threats.
HORIZON-CL3-2024-INFRA-01-02	Resilient urban planning	Secures urban infrastructures targeted by hybrid actors.
HORIZON-CL3-2024-FCT-01-07	CBRN-E detection capacities	Enhances law enforcement's ability to counter CBRN-E threats used in hybrid operations.
SU-INFRA01 (2018–2020)	Protection of critical infrastructure	Combines physical/cybersecurity measures against dual-nature attacks.
SU-GOVERNANCE (2020)	Countering radicalization on social media	Tackles disinformation campaigns used by hybrid threat actors.

Source: Analysis performed by the author, supported by Artificial Intelligence; ChatGPT. chat.openai.com/chat. 23 Feb 2025. Model: o1 pro.

The alignment of civil and defence challenges, as well as the concepts of civil preparedness and systemic resilience[40] themselves, should reshape the way modern security and defence threats are understood and addressed with dual-use R&I and should be recognised as a strong argument for enhancing synergies between civil and defence R&I. Similar conclusions are presented in the report of the Horizon 2020 Protection and Security Advisory Group (PASAG) highlighting that '*the prerequisite for promoting synergies […] lies in identifying areas/domains of reciprocal interest for both security and defence users*'[41]. The alignment on the critical infrastructures can both serve as a first step to "improve synergies between the areas of common interest of the security and defence programmes[42]" as well as a foundation for long-term strategic coordination with respect to dual-use R&I in these relevant domains.

Importantly, also investments of VCs specialised in defence technologies "span far beyond the battlefield, encompassing sectors like aerospace, supply chain management, and cybersecurity"[43]. The same applies to the recent proposal for the creation of a defence, security, and resilience bank as a multilateral lending institution[44].

The shared problem space and threat landscape mean that civil and military sectors, must develop similar capabilities to effectively respond to the common challenges particularly targeting critical infrastructures. This also underscores the need to "strengthen links between the defence industry and other strategic industrial sectors that are part of the same ecosystem, such as naval/shipbuilding, space, and aerospace"[45].

[39] Analysis supported by Artificial Intelligence; ChatGPT: chat.openai.com/chat. 23 Feb 2025. Model: o1 pro.
[40] Cf. NATO (2024), 'Resilience, civil preparedness and Article 3'.
[41] European Commission (2020), *PASAG report 2 -2020 – Dual-Use for Security*.
[42] *ibidem*.
[43] Bower (2024), 'Venture Capital Investment in US National Security'.
[44] This bank would offer low-interest, long-term loans to support essential national security priorities, including rearmament, defence modernisation. Cf. European Parliament (2025), Resolution on the Future of European Defence.
[45] The defence sector forms part of a broader strategic industrial ecosystem that relies on similar or interchangeable raw materials, technologies, skills, machines, and other industrial infrastructure,

1.3. Key barriers to civil-defence cross-fertilisation

1.3.1. Lack of sufficient funding and targeted support

The lack of sufficient funding and dedicated R&I programmes for supporting radically new technologies at low TRLs, all the way up to the maturation of technology and scaling up (higher TRLs), presents a major challenge for companies developing dual-use technologies[46]. While funding constraints exist in both the civil and defence markets, they are especially problematic for companies with disruptive and deep tech innovations seeking commercialisation in the defence sector. As demonstrated by the Survey, conducted by the author, many civilian technologies with dual-use applications are already available on the market or well advanced in the R&I process and can be adopted and transferred to address the defence and resilience needs, at the same time enhancing competitiveness of EU industry. This could save not only the time needed to develop the technology, but also the associated costs.

The surveyed startups and SMEs identified several civilian critical technologies-based solutions they developed, which they consider having dual-use significance, including examples, such as advanced battery technology based on aluminium metal for energy storage and electric propulsion; high-performance computing (HPC) and edge computing for enhanced processing capabilities; mobile network operator (MNO) infrastructure and private 5G networks for secure communication; synchronisation and inertial positioning, navigation, and timing (PNT) systems; interconnections and cabling solutions tailored for the quantum market; hyperspectral imaging technology capable of precise material detection; quantum cryptographic key exchange over optical fibre or satellite networks; software-based deep space radar systems; neuromorphic technology designed to enable AI processing at the edge; versatile aerial platforms capable of lifting heavy payloads. The survey illustrates that these primarily civilian technologies have a strong dual-use potential.

Furthermore, companies willing to develop dual-use defence-oriented solutions face significant difficulties in accessing EU funding programmes such as Horizon Europe, including for example European Innovation Council (EIC), given its exclusive focus on civil applications[47]. Moreover, many investors as well as financial institutions still impose explicit restrictions on dual-use companies regarding CAPEX requirements. Additionally, the difficulty of accurately assessing the defence market in the EU deters some VCs from investing in dual-use companies. As a result, many companies lack access to dual-use-oriented funding and decide to first develop their technology for civilian use to align with available funding opportunities. Furthermore, the European Defence Fund is perceived by some of the surveyed companies as favouring larger companies and consortia and prioritising incremental rather than disruptive innovations. This results in a situation where smaller companies developing dual-use innovative solutions have very limited financial options within the EU financial framework to offer solutions for military use. The barrier has recently started to be addressed at the EU level for example with the creation of the EU Defence Innovation Scheme (EUDIS) Business Accelerator, aiming at strengthening innovation within the European defence ecosystem which will recruit companies operating within the European defence industry or looking to enter it to be part of dedicated acceleration programmes with "onsite defence-focused bootcamps and unique learning and networking opportunities with defence end-users, industry representatives and investors, access to state-of-the-art testing facilities to speed up product development and technical coaching"[48]. Exemplary relevant topic areas of interest for EUDIS Business Accelerator have dual-use character, including autonomous systems (land/air/sea), AI-assisted mission planning & operation solutions, enabling AI on edge (HW & SW), advanced sensors and sensor fusion, next generation communications, AI threat

[46] Draghi (2024) also recommends that 'European funding for R&D is both increased and concentrated on common initiatives. This approach could be developed through new dual-use programmes and a proposed European Defence Projects of Common Interest to organise the necessary industrial cooperation'.

[47] 'A big problem for dual-use technology development is that Horizon, EIC and other instruments forbid the financing of such products', a quote from the Survey.

[48] European Commission, EUDIS Business Accelerator, available at: https://www.eudis-business-accelerator.eu/programme.

detection and defence, quantum encryption for secure military communications, wearable biosensors, portable life-support units, autonomous evacuation, automated triage and predictive casualty management, clean technologies, biotechnologies[49].

1.3.2. No market signalling

There is a lack of openness to innovation coupled with a lack of risk-taking culture within the defence sector and the broader public sector (i.e. the end-user), which leads to a deficiency in understanding the applicability of innovative solutions to civilian and defence needs and challenges. The Survey indicates that this is particularly true within the defence realm. '*Business opportunity is unclear. It easily means wasting time to go after defence, because it is so unclear if my technology will actually be interesting*'[50]. *'More challenging is to secure projects with the military to demonstrate the technology because of military conservative approach to civil technology. We believe more demonstration projects are required, and the military should be encouraged to look more in the civil market for existing solutions and request and fund demonstration projects and work together to analyse how it can be used in defence context as well. We are engineers and we can make things work but we need inputs and requirements about use cases and to learn more about challenges from the military. The military could spend more funds to explore and demonstrate projects of technology with dual-use case potential'*[51].

As a result of this 'conservative' posture, there is no effective market signalling possible from civil to military sector, hindering the presentation of market offerings, as well as reverse signalling regarding end-user requirements and capability demand. What is needed is the application of the open innovation model[52] that could lead to translation of operational needs into capability requirements, which can be addressed by dual-use non-traditional providers through R&I processes within acceleration programmes designed similarly to DIANA, or DARPA and ARPA-style challenges, whose goal is to acquire solutions for defined capabilities.

1.3.3. Lack of acceleration and testing support

Dual-use R&I activities performed by academic and business stakeholders require specific support, with access to research facilities, innovation hubs, and accelerators. This was confirmed both by the Survey as well as by Commission's public consultations on EU Startup and Scaleup Strategy[53]. However, in Europe, there is only a limited number of well-structured acceleration programmes such as for example EUDIS Business Accelerator, mentioned above. These programmes are essential especially for meeting defence needs and system and operational requirements by supporting the testing, validation, and demonstration processes in military settings hardly available for commercial use —such as field testing with professional military experimentation units on specialized defence test beds, and defence sandboxes (including free-flying zones, jammable areas, large Radio Frequency ground stations, simulation and wargaming IT systems). Additionally, some dual-use disruptive technologies, such as quantum technology, have unique requirements regarding testing and validation. According to the Survey, conducted by the author, quantum computing development would significantly benefit from a collaborative testbed that allows for the integration and optimisation of the best components. Currently, most quantum technology developers conduct in-house testing, which slows progress unnecessarily. There are only a few technologies that do not face these problems, at least according to the Survey results. These include energy and cryptography, where products and requirements are relatively similar in both civilian and defence markets.

---

[49] *Ibidem*.
[50] A quote from the Survey.
[51] A quote from the Survey.
[52] European Commission, 'Open Innovation 2.0 and Horizon2020: Opportunities and Challenges'.
[53] European Commission (2025), 'European Commission concludes public consultation on the EU Startup and Scaleup Strategy'.

1.3.4. Lack of data

There is a significant need to obtain diverse datasets for R&I purposes, particularly for training of AI/ML algorithms[54]. Researchers and companies are facing difficulties in accessing different types of data in all critical technology areas. That is particularly challenging for dual-use R&I projects needed to train their algorithms for defence applications, as these data sets are almost impossible to access, and civilian data are not relevant. These include: data for logistics systems, technical status of equipment, resource consumption (e.g., fuel, ammunition), warehouse/stock levels and logistics management, images/videos – regardless of the origin: satellite, aircraft, including UAV, land and maritime platforms – visual, thermal/infrared, multispectral imaging, remote sensing, radar/SAR (Synthetic Aperture Radar), 3D models of terrain and objects, point clouds, sensory data, environmental sensors, meteorological (weather forecasts, e.g., temperature, wind, humidity, precipitation), chemical data (air, water composition and pollution), radiological data (radiation levels), inertial sensors (e.g., for drone and vehicle navigation, weapons systems stabilisation, traffic monitoring), force and combat data.

1.4. Benefits of dual-use R&I

Mitigating the risk of failing into the "valley of death"

Pursuing a dual-use R&I model provides startups with a strategic advantage by mitigating the risk of falling into the "valley of death"— a challenge that disproportionately affects companies worldwide developing solutions solely for the defence sector. It is also reinforced by the characteristics of the EU defence market which is characterised by oligopolistic structure with a high degree of market concentration, where large, established defence contractors benefit from a comparative advantage of having the capacity to comply with complex public procurement procedures, security requirements, and complex defence standards. In contrast, commercial companies, especially SMEs and startups, often referred to as non-traditional providers, struggle to overcome these challenges and numerous barriers when attempting to enter and compete in the defence market.

Given the structural barriers in defence procurement, administrative burdens and inherent characteristic of the defence sector, which favours large, established players, as indicated in the Survey startups face significant difficulties in securing contracts within a timeframe that allows them to financially sustain their operations through the commercialisation phase. '*What kills technology transfer is primarily the speed. It is hard to stay afloat for 2-4 years before a deal is made due to ultra-long sales cycles. If a decision—whether yes or no—was reached faster, it would make a world of difference for the ecosystem. DIU or Cyber Innovation Hub in Germany are good examples of how this challenge can be tackled*'[55]. Sales cycles to secure government contracts can extend over several years, and navigating this "valley of death" is often hampered by lengthy approval processes and bureaucratic obstacles. For that reason, having parallel civilian applications that sustain a company's growth and the technological maturation of its solutions, while also supporting early references and achieving market validation, is a strategic approach to overcoming these challenges as well as benefiting from broader market opportunities - which is yet another advantage of dual-use R&I model. Usually, however, start-ups (and SMEs) act as technology/components providers in primes' (systemic integrators') value chains, which, in fact, should be beneficial for both. Commercial path of technology development can prevent start-ups from a brain-drain and being absorbed, allowing to grow.

[54] The problem of 'the creation of large, integrated data sets for training AI models' was also pointed out in Draghi (2024).
[55] A quote from the Survey.

Broader market opportunities

According to the Survey results, civilian market has a '*larger market potential to attract outside investment*'[56] and R&I funding opportunities. One of the startups surveyed explicitly pointed out that '*whilst our technology has applications in the defence space natively, defence alone would not be able to supply a significant market in comparison with civil mass markets such as telecommunications. Similarly, whilst during the academic research phase of this technology we received funding from defence funding bodies, the majority of governmental grants are aimed at civil applications*'[57].The Survey helped to observe that the successful strategy of many defence newcomers started with the R&I process focusing on civilian application supported by better funding opportunities of technology for civil use, and parallel identification of defence applications which were further developed in collaboration with end-user and later funded within available funding schemes (both civil- and defence-oriented).

Companies that choose to develop solutions with dual-use applications and position themselves within a broader security context e.g., public safety, disaster response or within large market sectors such as telecommunication, financial system (banks), healthcare, administration, logistics will gain access to broader market opportunities of civilian and military sectors. This can enhance their financial efficiency, including higher returns on investments such as VC funding in technology. The fact that the '*dual-use approach also enhances a company's attractiveness to investors by offering a diversified portfolio that mitigates risks associated with dependence on a single market*' is also confirmed by well-established companies' experience[58].

However, drawing this conclusion requires a disclaimer, that when a critical technology is mature, in some cases, it may be more efficient to choose a sector of application, rather than pursue dual-use applications. That finding suggests that, within a diversified portfolio of critical technologies and their respective product and solution applications, there is no one-size-fits-all strategy or model. Certain cases may not be aligned with all findings making the dual-use R&I conditions even more complex.

Time to market

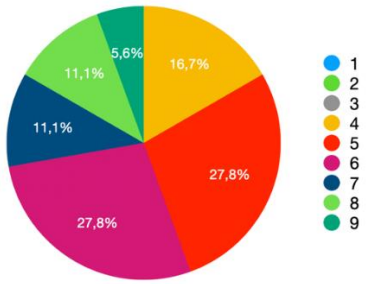
The dual-use R&I model could be even more effective if civil-defence synergies were developed at the early stage of the process. Early identification and validation of dual-use applications done with a potential end user, along with investment in a dual-use R&I path, can significantly accelerate time to market. If a startup initially follows only the civilian development track, it may later face significant barriers in transitioning to dual-use applications. Startups that focus exclusively on civilian applications, but are willing to enter dual-use path, often find themselves having to scale down or reengineer their solutions to integrate defence-specific requirements later in the R&I process, which can be costly and time-consuming. The results of the Survey and interviews indicate that, in practice, the most suitable phase of splitting development paths when synergies often emerge is reportedly between TRL 4-6 (72,8% of respondents of the Survey from the business sector). But it is worth being noted that some researchers suggest that '*synergies are possible only at early research phases (TRLs 1-4) when research is still 'application-neutral*'[59]. Both findings, however, are critically important to highlighting that synergies occur primarily at the early stage of the R&I process, which is also confirmed by the PASAG Group stating that '*technologies with lower TRL (…) are loosely related to the field of application ("application agnostic"), and therefore their potential for dual use is higher*'[60].

Interestingly, the European Preparedness Union Strategy stresses the importance of promoting dual-use by design, including for technologies[61]. Under such a "dual-use-by-design" model, a project or a company could pursue—where appropriate and cost-effective in the long term—a

[56] Survey with Icewind, available at: https://icewind.is/.
[57] Survey with Aquark Technologies, available at: https://www.aquarktechnologies.com.
[58] Addionics (2024), 'Unlocking Market Opportunities with Dual-Use Technologies'.
[59] Fiott, and Ketselidis (2022), 'EU Civil-Defence Synergies: Understanding the Challenges and Drivers of Change'.
[60] European Commission (2020), *PASAG report 2 -2020 – Dual-Use for Security*.
[61] European Commission (2025), *Joint Communication on the European Preparedness Union Strategy*.

simultaneous alignment with both civil and defence requirements, or unified requirements. This would ensure that only minimal modifications would be needed to adapt a given technology to civil or defence standards when targeting the respective market. At higher TRL levels, this would require a political decision to unify design standards or to develop so-called "hybrid standards"[62], and could be applied to at least some hardware of software components, or relatively new technologies, such as AI - a foundational technology, which is critical for both civil and defence solutions, that has not yet established applicable standards. For example, one of the ideas which has been circulating within the expert community is to focus on setting up '*universal standards for dual-use AI in the military context*'[63], which, perhaps, could be integrated with the standard setting process of the civil sector. Experts have argued that '*the lack of such standards exacerbates risks, including ethical practices, regulatory gaps*'[64].

Figure 2: What is the critical TRL* at which technology development should begin in dual-use mode or transition from a civilian to a defence (or vice-versa) application track?



Source: Survey by the author, February 2025.

*TRL stands for Technology Readiness Level.

***The survey sample included 80 respondents, out of which 24 (30%) replied. An explanation of the survey sample is provided in the methodological section of this chapter.*

Enhancing cost-capability ratios

The economy of war in Ukraine has proven that the civilian origin solutions applied to defence purposes can occur to be cost-effective enhancements to its defence systems. Well-known and game-changing examples include reconnaissance and adaptable weaponry capabilities include (but are not limited to):

- Low-cost commercial drones, such as the DJI Mavic, available for just USD 2 000 and used to targeting or engaging large, heavy and expensive military systems (armoured vehicles, radars and communication, artillery, and even airborne targets);
- Naval drones (such as e.g. Magura family, being in fact rebuilt water scooters equipped with explosives and communication devices costing USD 250 000), deployed against Russian Black Sea Fleet warships;
- New satellite communication capabilities provided by Starlink; and artificial intelligence solutions, such as Palantir's AI-enhanced software improving targeting accuracy or

[62] 'There will then always be a need to have land, air and naval assets, but the onboard components of such capabilities increasingly derive from technological advances made in the commercial sector. It is for this reason that 'hybrid standards' have become crucial in efforts to ensure that defence and security actors can freely and effectively use commercially developed technologies', see more: Fiott (2014), 'The three effects of dual-use: Firms, capabilities, and governance'.
[63] Albrycht et al. (2024), 'Dual-use Technology – Cross-sector cooperation in the cyber security sector'.
[64] A quote from the Survey.

Primer's AI-trained software adapted to extract actionable intelligence from unencrypted Russian radio communications[65].

Bridging the innovation gap and generating spin off effects

The increasing interest of private VC investments in the dual-use technology sector is an opportunity to bridge the innovation gap between rapidly evolving defence requirements—driven by dynamic battlefield changes—and the security and defence sectors' limited budgets for innovation, very often due to overall underinvestment of armies and modernisation backwardness. This investment trend can play a crucial role in fostering innovation and transforming R&I processes into more agile and capability-driven ones, ensuring they address the real needs and challenges faced by security and defence end-users, leveraging "legacy" equipment features (excellent cos-effect ratio). This trend can also have the reverse impact on the civilian sectors with the spillover effect with diffusion from defence to commercial applications (spin offs) and advancing the competitiveness of several industrial sectors.

It is already interesting to observe the emerging reverse pattern of technology transfer in Ukraine, where defence technologies are beginning to be adapted for civilian and security applications, enhancing safety, efficiency, and quality of life across both public and private sectors. Advanced sensors, drones, and mapping tools designed to provide battlefield awareness Intelligence, Surveillance, and Reconnaissance (ISR) have been adapted for environmental monitoring, wildlife conservation, urban planning, and search and rescue operations. Robotics initially created for hazardous material handling, reconnaissance, or unmanned logistics can be repurposed for industrial automation, agriculture (e.g., autonomous tractors), urban delivery services, and even medical robotics (such as surgical assistants). Military logistics systems, designed to operate under extreme conditions, have informed advances in supply chain management, including inventory tracking, rapid distribution networks, and route optimisation tools for humanitarian aid and disaster relief. Portable power generation and energy storage systems developed for field operations can be used in off-grid communities, emergency relief efforts, and renewable energy applications for civilian infrastructures. Virtual reality, augmented reality, and simulation systems originally created for military training can be adapted for civilian education, medical training, industrial safety simulations, and even complex system modelling in urban planning. High-performance materials engineered for soldier protective equipment can be employed in constructing safer buildings, manufacturing sports equipment, enhancing automotive safety, and producing lightweight, durable personal protective equipment (PPE) for various industries. Filtration, sensor, and detection technologies used to monitor chemical or biological threats on the battlefield can be repurposed for improving air quality in urban centres, industrial safety monitoring, and public health surveillance.

1.5. Risks related to dual-use R&I

Dualism of standards and requirements

Even though the successful dual-use model would increase the chances of certain technology or solution to succeed in both markets, under current legal and regulatory conditions, it may still - but does not have to[66] - face risks of higher costs, longer time to market and slower innovation. This is particularly related to the need to simultaneously satisfy both civil market requirements, as these requirements serve very different needs (economic on the one hand, security/defence on the other) and to comply with more extensive defence standards. That is why considerations regarding systemic changes are now part of the political discussion on enhancing dual-use R&I and could further be addressed at both national and EU levels. For example, some of these risks were recognised and addressed in the *Joint White Paper for European Defence Readiness 2030*, which

[65] Grace, Egan, and Rosenbach (2023), 'Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S.'.

[66] It was supported by the Survey results showing that different startups and SMEs have different perspective on the risks and assessment of their significance.

states that the EU '*can add value by using uniform design standards for dual-use and defence and security capabilities*'[67].

Export control compliance risks

Dual-use R&I is a subject of extensive and complex export control compliance measures of EU and national dual-use export control regulations that requires for example to implement Internal Compliance Programme (ICP)[68]. These legal requirements introduce additional administrative overhead and can significantly prolong development cycles of dual-use R&I projects as well as impose higher costs, in contrast with the expected benefits. The risk of complex export controls was confirmed by the results of the Survey which highlighted that as one of the barriers limiting the ability to develop or commercialise technology. The lack of in-house expertise, the resources or experience in navigating regulatory landscapes poses a substantial barrier for startups as persistent investment restrictions and export controls can be complex. Encompassing that risk, the Commission has released guidance "to help researchers and research organisations to identify, manage and mitigate risks associated with dual-use export controls and to facilitate compliance with the relevant EU and national laws and regulations"[69]. The complexity of the topic is widely covered in chapter 2.

Security challenges and threats

As the Survey results confirmed, '*security is a must in dual-use applications*'. That is why, another important risk that should be highlighted are complex security challenges and threats faced by stakeholders involved in dual-use R&I projects. First of all, the dual-use R&I affiliated risk is the exposure of the project's intellectual property to confidentiality threats, including insider threats and cyberespionage. Given that a significant number of dual-use and deep-tech projects originate in the academic sector, which faces a high volume of external cyberattacks, there is a high risk that the confidentiality and integrity of sensitive research data, including groundbreaking research results and technological innovations made by the scientific community, could be compromised[70] potentially undermining both national security and the commercial viability of technological solutions. Data from the Checkpoint report is alarming: '*the Education/Research sector was the most targeted, with an average of 3,828 weekly attacks, followed by the Government/Military and Healthcare sectors, with 2,553 and 2,434 attacks, respectively*'[71]. These findings are corroborated by the Verizon's 2024 Data Breach Investigations Report, which highlights that the education sector '*was by far the most impacted, accounting for more than 50% of breached organisations*'[72]. The report analysed 30,458 real-world security incidents and confirmed a record-high number of 10,626 data breaches, with 1,537 cases of confirmed data disclosure in educational services[73].

This has led to a critical need to significantly enhance cyber-resilience across the entire academic science but also technology sector including SMEs and startups which facing the same types of cyber threats but in the smaller scale. This should include the implementation of specific preventive measures, information classification protocols and secure data handling procedures, as well as education and training of researchers and innovators. Since cyberespionage has a significant impact also on economic competitiveness, these measures should be in fact implemented regardless of whether the applications are dual-use or purely civilian. For the security of dual-use R&I activities and the security and integrity of dual-use solutions, it is also particularly important to establish a secure supply chain (without any dependence on non-NATO countries components). However, as the Survey results suggest, '*for startups it is not easy to recognize each component*

[67] European Commission (2025), *Joint White Paper for European Defence Readiness 2030*.
[68] European Commission, 'EU compliance guidance for research involving dual-use items'.
[69] *Ibidem*.
[70] Albrycht, 'Cyberthreats to the Science and Research Sector as a Challenge to National Security and Economic Competitiveness'.
[71] Checkpoint (2024), 'A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide'.
[72] Verizon (2024), '2024 Data Breach Investigations Report'.
[73] *Ibidem*.

origin and track the whole supply chain'[74] as well as '*to maintain a whitelist of collaborators or customers'*[75] which can lead to the security risks if not well addressed.

The third challenge is the need to establish secure development environments with high-security zones, restricted access.

The fourth one is the need to engage personnel with security clearances in dual-use R&I. Based on the Survey and Interviews, talent constraints are an important challenge in dual-use R&I projects, i.e. due to the scarcity of professionals with both technical expertise and the required security clearances – which may lead to substantial workforce limitations. Many skilled engineers and researchers may not want to or may not be eligible to work on sensitive projects immediately, and the clearance procedures are time consuming varying from 6 up to 18 months in different EU countries.

Supply chain challenges

Companies dealing with critical technology R&I which has dual-use potential are facing challenges in the value chain due to the limited availability of enabling components. International geopolitics and trade protectionism have made it difficult to buy high-end components which causes European technology to lag behind (e.g. U.S. export controls on Field-Programmable Gate Arrays, which are essential for most quantum technologies). One respondent even suggested that issue is in fact related to a lack of manufacturing capabilities in EU: '*We require funding to build our own chipfab(s). We need to control this infrastructure ourselves to not be slowed down but lack access to required growth funding (and electricity and permits take too long!)*'[76].

[74] A quote from the Survey.
[75] A quote from the Survey.
[76] A quote from the Survey.

2. Practical implementation of dual-use R&I

2.1. Introduction

Defining dual use is challenging and various dichotomies have already been attributed to the term: civilian and military use, defensive and offensive use, peaceful and non-peaceful use, and constructive and destructive purpose[77]. In addition, the term is often linked to intended uses (beneficial) and unintended uses (detrimental use or misuse). The intention of dual-use technologies is often to serve peaceful or commercial purposes. The usefulness of dual-use items lies in their versatility. Due to their inherent capabilities, they can be adapted or repurposed for use in military, security or human rights violation applications.

The dual-use terminology is being used with different meanings complicating a straightforward understanding in the context of R&I:

- In a first dimension, it is a broad view on the *inherent dual-use nature of many general-purpose technology*[78]. Technology domains such as semiconductor technologies, quantum technologies, biotechnologies and artificial intelligence technologies are generic and can address the needs of both civil and military users, even though at a given stage of technology maturity the field of application is not yet known.
- In the second dimension, dual-use R&I refers to activities involving *dual-use technologies with the potential for civil-defence synergies*, and thus for the benefit of both sides. This, for example, concerns niche innovations where the emphasis is on identifying and pursuing civil and defence use cases that are relevant for contributing to societal, global, industrial competitiveness and security challenges. The synergy should preferably work in two directions: on the one hand, commercialising defence technology for civilian purposes, and on the other hand targeted uptake of innovative solutions from civil applications to defence use.
- In a third dimension, dual-use R&I can refer to the involvement of technologies during the research activities that has the potential to be used for both civil and military purposes. In its narrow understanding, it refers to *dual-use items (goods, software and technology) that are subject to EU Regulation 2021/821*, setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual use items[79]. This is, in essence, a trade control regulation for sensitive, strategic items with national security, terrorism or human rights considerations. Commission Recommendation (EU) 2021/1700 provides guidance on dual-use export controls for the research sector and uses the terminology 'research involving dual-use items'. In this third dimension, the term dual-use R&I refers then to 'research involving dual-use items'[80]

Dual-use R&I described in the first and second dimension can be impacted by export controls described in the third dimension.

Export controls require controlled items (goods, software or technology) and controlled activities (exports, transfers, brokering, transit, provision of technical assistance, but no imports). Authorisation applications involve screening of the transaction items, involved parties, stated or suspected end-use and country of destination. Export controls are traditionally geared toward

[77] Sánchez Cobaleda (2020), 'Definitions of concepts: Dual-use goods'.
[78] Alternative names include foundational technologies, emerging technologies or critical technologies.
[79] 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.
[80] Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

restricting the physical transfer of sensitive technologies, but do not exempt research output meeting the control thresholds.

Dual-use controls impose restrictions, not *per se* prohibitions, on the trade or flow of sensitive items (goods, software or technology), largely destined outside the EU. The scope is intentionally targeted and restricted in scope. Transactions or collaborations involving items not listed, but subject to end-use and end-user controls of concern can only be subject to export controls after some cumulative conditions are met. The EU dual-use export control system provides a legally binding framework at the EU level, and it is implemented by export control authorities in each EU Member State.

The overall impact of dual-use export controls in general should not be overstated. Key data provided by the European Commission and EU Member States indicates that the total number of dual-use licences was 138,764 in 2022, which mounts up to 2% of the value of total extra-EU exports of goods. In the same year, the total number of dual-use denials was 813, corresponding to 0.04% of the value of extra-EU exports of goods[81,82].

Assessing the impact of export controls in an R&I context is not straightforward in the current setting. On the one hand, no export control relevant data is gathered by the funders. The main reasons are:

- the explicit choice in the transition from Horizon 2020 to Horizon Europe funding programme not to request a declaration of the dual-use character of the project based on an ethics self-assessment and to not insert it elsewhere (scientific review, security scrutiny or third country control, if applicable).
- the Horizon Europe application process, including application form, grant agreement and consortium agreement, assigns the responsibility for compliance with the export control requirements to the applicants and does not prescribe an export control review when needed, even when the proposal clearly involves potentially listed dual-use technologies such as cryogenic technologies, space propulsion, hyperspectral imaging for remote sensing.
- neither a general, nor a targeted requirement for Horizon Europe proposals or projects to provide evidence of an export control check.

On the other hand, there is no systematic data collection at the side of the export control authorities in the EU to assess the impact of export controls on dual-use R&I:

- The annual reports of the European Commission on the implementation of the EU dual-use regulation illustrate that there is (very) limited information available outside the realm of export control authorities to assess the impact of export controls (such as number of licences, number of denials, etc.) according to the typology of exporter, such as small and medium-sized enterprises (SME) or research organisations.
- No data is available or collected whether a licence application was received, or a licence was granted or denied in the context of a research project, funded by Horizon Europe.
- Interestingly, the latest report from 30 January 2025 refers to dialogues between Commission services responsible for export controls and for R&I funding, which is a possible way forward for further dialogues on the intersection between both policy areas to improve awareness and relevant guidance on the impact of export controls for funded research involving dual-use items[83].

[81] This includes voluntary data provided by the EU Member States on the uses of National General Export Authorisations and EU General Export Authorisations.
[82] European Commission (2025), Report on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.
[83] European Commission (2025), Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

Currently, there is no evidence or sufficient data to assess Horizon Europe projects' compliance with dual-use export controls. It is however likely that an in-depth screening of granted projects will discover dual-use R&I that was/is/will be subject to dual-use export controls. The percentage, when identifiable, will remain low compared to the total amount of granted projects. Given the expected rise in projects to be funded in the coming years involving dual-use technologies or exploring civil-military synergies, seeking for a better methodology to identify and track these projects becomes paramount.

This chapter has two main parts: the first part focuses on research performing organisations and the second part emphasises on the SMEs, start-ups and scale-ups.

2.2. Research performing organisations

2.2.1. Background

The first part of this chapter focuses on the practical implementation of dual-use research and innovation by research-performing organisations (RPOs) within EU-funded project with a civil focus. In this context, 'dual-use research' refers to research projects involving dual-use items, which under the Commission Recommendation (EU) 2021/1700 specifically includes "dual-use items that are used during research or research that results in research output in any possible form meeting the technical specification of a dual-use item in the EU dual-use control list or in a complementary national dual-use list (if any)."

In certain research or field—particularly those with civil-military synergies or those focused on cutting-edge technologies—there is a risk that sensitive knowledge, technology, or research outputs could be misused. While research may be conducted for legitimate civil purposes, unintended transfers or illicit final uses could lead to military applications, or other applications that threaten human rights or public security. Export controls, or more broadly, trade controls, serve as a mechanism to regulate such transfers and mitigate these risks.

The EU regulates the trade and transfer of dual-use items under Regulation 2021/821, which consolidates and updates previous versions. Historically, EU export control policies have been primarily industry-focused, with the supporting infrastructure developing accordingly. However, as awareness of the implications for research has grown, the EU has made increasing efforts to provide clarity and guidance to research organisations. The regulation has always defined an "exporter" broadly to include any natural or legal person, meaning that researchers and RPOs have technically been subject to these controls for years[84]. However, only in the latest and consolidated revision are academic and research institutions *explicitly* acknowledged as stakeholders, with Recital 13 of the above-mentioned Regulation recognising their unique challenges—largely due to their commitment to the free exchange of ideas and their involvement in cutting-edge technologies.

Despite being subject to export controls, many RPOs have only recently started to develop more structured compliance processes[85]. Cases of enforcement within academia and research have increased in visibility, leading institutions to reassess their responsibilities. Under the regulation, an EU researcher may be subject to controls if he/she transfers dual-use items to non-EU countries or, in some cases, to non-EU nationals or temporary residents within the EU. This applies to tangible transfers—such as shipping specialised equipment for testing—as well as intangible ones, including sharing controlled technical data via email, collaborating with non-EU researchers, or providing technical assistance at webinars or international conferences.

Non-compliance not only may carry legal and financial penalties but also undermines the core objective of export controls—preventing the proliferation of goods and technologies that could be used for military applications, human rights violations, terrorism or threats to public security.

[84] For the evolution of the EU dual-use Regulation over the years, see: Colussi (2024), 'The evolution of the EU STC system'.
[85] Cf. CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper'.

However, while these risks demand close and high attention, dual-use transfers represent a relatively small fraction of total extra-EU exports (about 2% as per latest data from 30 January 2025)[86], making this a unique area where lowest-volume transfers require the highest level of scrutiny and control.

EU and national authorities have increasingly recognised the complexities of applying export controls in a research context. While national authorities may have well-established expertise in regulating the export of physical goods, their familiarity with technology transfers in academic and research settings is in some case still developing[87]. This gap has contributed to uncertainties in how EU research organisations should implement compliance measures.

Recognising these challenges, the EU published its first dedicated recommendations on export controls in research in 2021[88]. This document provides information on how export controls apply to dual-use research and outlines steps for implementing an internal compliance programme (ICP)—a concept formally introduced in the Regulation 2021/821[89], where it became a requirement for obtaining certain licenses[90]. In parallel, additional EU guidance has addressed foreign interference risks[91] and research security[92], reflecting a broader effort to balance scientific openness with geopolitical and security considerations.

Stakeholders have noted that researchers and RPOs who were previously encouraged to collaborate globally—particularly in emerging and key-enabling technologies—now face new compliance expectations. These extend beyond academic and research concerns, intersecting with political and economic security issues[93].

As a result, tensions can arise between export controls and the principle of academic freedom, leading some researchers to question whether these regulatory provisions should apply to their work. Scientific freedom is a universal right and a public good[94]. It is a fundamental principle of the EU and, as such, is deeply embedded in the EU Charter of Fundamental Rights[95]. However, recent geopolitical events—including the COVID-19 pandemic, Russia's war of aggression against Ukraine, conflicts in the Middle East, and growing technological competition— have placed significant pressure on the notion of openness in research. In response, the EU has sought to maintain a delicate balance, promoting open research while implementing necessary restrictions to safeguard security, innovation, and international cooperation. While challenges in implementing export controls affect research more broadly—extending beyond EU-funded projects to the wider academic and scientific landscape—finding concrete and targeted solutions may be more feasible within the structured framework of EU-funded projects. This setting offers a defined regulatory and operational space where clearer guidance, standardised procedures, and dedicated support mechanisms can be introduced to mitigate uncertainties and administrative burdens.

This part of chapter 2 first outlines its scope and objectives before detailing the research methodology, including the selection of stakeholders and key areas of inquiry. The main body

---

[86] European Commission (2025), Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

[87] Cf. European Export Control Association for Research Organisations (2024), 'Feedback on the White Paper on options for enhancing support for research and development involving technologies with dual-use potential', Position paper.

[88] Commission Recommendation (EU) 2021/1700.

[89] Regulation (EU) 2021/821.

[90] According to Article 12.4 of Regulation (EU) 2021/821, exporters using global export authorisations shall implement an ICP, unless deemed unnecessary by the competent authorities. Furthermore, an ICP is a requirement to apply for the Union General Export Authorisation No. EU007.

[91] European Commission (2022), 'Tackling R&I foreign interference'.

[92] Council of the EU (2024), Recommendation of 23 May 2024 on enhancing research security.

[93] CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper', p. 22.

[94] Ministerial Conference on the European Research Area (2020), *Bonn Declaration on Freedom of Scientific Research*.

[95] Article 13 states: '*The arts and scientific research shall be free of constraint. Academic freedom shall be respected*'.

presents and discusses the findings, highlighting both the challenges encountered and potential measures to support dual-use research, as identified by stakeholders. Finally, it concludes with reflections on the insights presented.

2.2.2. Scope and objectives

The first part of this chapter aims to provide data and insights on the implementation of EU-funded research projects (Horizon Europe and Horizon 2020) by RPOs with an exclusively civil focus. It seeks to offer a deeper understanding of the involvement of dual-use items in these research projects and the associated challenges, serving as a foundation for evaluating the current system and informing future discussions on dual-use R&I. To achieve this, the chapter examines how RPOs address the issue during EU-funded research projects, highlights the most common and significant obstacles identified through stakeholder input, desk research, and literature review, and explores potential measures and strategies suggested by relevant stakeholders.

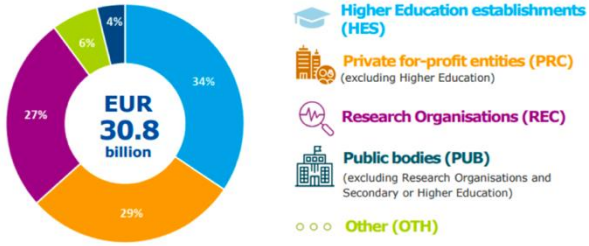
The specific objectives of the chapter are to:

- Map the stages in the lifecycle of an EU-funded project with an exclusively civil focus where dual-use issues may arise.
- Conduct a comparative analysis of how different RPOs handle these issues.
- Evaluate the effectiveness of past and current guidance on the topic.
- Identify key challenges in implementing EU-funded dual-use R&I research
- Highlight key areas for future attention, with the ultimate goal of helping researchers and RPOs conduct their activities while remaining compliant with applicable laws, particularly export controls on dual-use items.

To clearly define the scope of this research, it is important to specify that "RPO" here refers to any non-profit organisation engaged in research. This includes research institutes, higher education institutions, and academia. The recommendation on enhancing research security defines an RPO as "any non-profit organisation that performs scientific research."

RPOs play a vital role in advancing science, technology, and society. Within the Horizon Europe framework, RPOs are the leading participants in R&I projects, ranking ahead of industry and for-profit organisations[96].

Figure 3: Percentage of Horizon Europe beneficiaries, 2021-2023



Source: “Horizon Europe implementation, Key figures 2021-2023,” Directorate-General for Research and Innovation, European Commission, May 2024.

It is worth mentioning that RPOs and industry may sometimes differ in how they address dual-use research. Industry often benefits from longer experience in this area, as it has historically been the primary target of export controls. As a result, industry players may have more established compliance mechanisms and guidance from national and competent authorities. In contrast, awareness and expertise in export controls among many RPOs have emerged more recently.

[96] European Commission (2024), ‘Horizon Europe implementation, Key figures 2021-2023’.

Consequently, RPOs may face greater uncertainties regarding the implementation of these controls in a research context, concerning for example open-access publication, cloud storage, and making information available. For this reason, the chapter focuses specifically on RPOs, as defined in this context, ensuring that their perspectives and insights are not mixed with those of other organisations that also conduct research and participate in EU-funded projects, but may differ in their core business, principles, understanding, and approach to the issue.

The EU and national governments are actively addressing export control challenges in a research context, engaging in discussions with RPOs, and demonstrating a willingness to provide support. However, the level of information and guidance available varies significantly across EU Member States[97]. Some governments have prioritised knowledge security and provide extensive guidance, while others have offered little to no direction.

When implementing and analysing the application of controls on research involving or resulting in dual-use items, it is crucial to consider the interplay between multiple factors, including export controls, academic freedom, openness in international cooperation, ethics, confidentiality, foreign interference, and economic security. Due to its complexity, dual-use export control compliance can be particularly challenging in an EU context, where responsibilities are shared between supranational and national authorities. However, it is also important to remember that, despite its significance, dual-use research constitutes only a small portion of EU research activities.

For research organisations, challenges extend beyond legal compliance with export controls; geopolitical factors and ethical considerations also play a role. Regardless of the specific application framework—whether an EU-funded project or another research initiative—challenges persist, but potential solutions are also available. While these challenges are broad, more targeted support and improvements can be identified in specific contexts, such as Horizon Europe projects. Additionally, tailored measures within this framework could help facilitate compliance and research activities.

2.2.3. Methodology

With regard to methodology, this chapter relies on a mixed-methods approach, incorporating both quantitative and qualitative data. Data were collected and analysed through a combination of literature review, desk research, interviews, surveys, and a dedicated group discussion with stakeholders from RPOs. The triangulation of data—combining different sources and methodologies—was used to cross-reference quantitative and qualitative findings, helping to reduce bias and provide a more comprehensive understanding of the field of inquiry. Quantitative analysis was employed to identify trends and patterns related to specific topics, while qualitative data collection and analysis allowed for a deeper exploration of survey responses and an examination of areas that remained unexplored in the survey.

In addition to first-hand insights gathered from stakeholders, the report builds on knowledge obtained from the analysis of primary and secondary sources, guidance documents issued by national and supranational authorities, stakeholder feedback from EU Commission consultations on dual-use items export control, and published documents, such as position papers from RPOs and related associations. Furthermore, high-level reports, including those by Heitor[98] and Draghi[99], as well as studies conducted by the Joint Research Centre (JRC) and other EU institutions and bodies, were taken into consideration and contributed to the development of this research.

Regarding interviews, stakeholders were identified through a structured methodology that drew on information from various sources and tools, including the Horizon Dashboard and the TIM-Dual-Use platform. These tools were complemented by additional data obtained through qualitative

[97] Countries like Germany have provided dedicated guidelines, such as BAFA (2023), 'Manual - Export Control and Academia'.
[98] European Commission (2024), *Align, Act, Accelerate: Research, Technology and Innovation to boost European Competitiveness*.
[99] Draghi (2024), *The future of European competitiveness: A competitiveness strategy for Europe*.

analysis of specific projects with dual-use potential. The Horizon Dashboard provided data on the top research organisations participating in Horizon 2020 and Horizon Europe projects, regardless of their involvement with dual-use items. Meanwhile, TIM-Dual-Use was used to identify research organisations that had published the most research potentially involving dual-use items within EU-funded projects since 2014, covering both Framework Programmes for R&I - Horizon 2020 and Horizon Europe[100].

By cross-analysing data from different sources with distinct scopes, a list of potential stakeholders for interviews was compiled. A total of 21 interviews were conducted between 4 and 21 February 2025, alongside a dedicated group discussion, organised on 17 February 2025. Interviewees held various roles, most often related to compliance, within different types of organisations. The interviews were semi-structured, aiming to understand how RPOs handle dual-use projects, at which stages they encounter dual-use challenges, what difficulties they face, and whether they had recommendations for improvement. Additionally, the effectiveness of past and current guidance on dual-use research was discussed.

The dedicated group discussion was conducted with Board Members of the European Export Control Association for Research Organisations (EECARO), an association recognised as a key player in the field of export control in research. EECARO is the first association of its kind in the EU, bringing together export control officers from research organisations across the EU and EFTA countries. It was established at the end of 2022 by five founding members from Belgium, the Netherlands and Germany[101].

Regarding the survey, it was designed to gather insights into key areas, including:

- The perceived administrative burden when dual-use items were involved in research.
- Whether dual-use concerns had ever prevented participation in EU-funded projects or led to project discontinuation.
- Challenges in implementing export controls in EU-funded projects.
- The stages of a project where dual-use issues typically arise.
- An assessment of the effectiveness of past and current guidance.
- Gaps in the current system and possible solutions or improvements.

The survey consisted mainly of closed-ended questions, with opportunities for respondents to provide additional comments and input. It was distributed through various channels, primarily associations of RPOs with varying levels of expertise and focus on the topic. Key distribution partners included EECARO, the European Association of Research and Technology Organisations (EARTO), the European University Association (EUA), the League of European Research Universities (LERU), and The Guild of European Research-Intensive Universities.

The survey was conducted between 6 and 22 February 2025 and received 38 responses. Of these, 19 came from universities, while the remaining responses were from other types of research organisations, such as national institutes for technology, independent nanoelectronics R&D hub, and organisations focusing on applied research, technology and innovation. The organisations represented in the survey are from both EU and non-EU countries, including Austria (3), Belgium (7), Denmark (2), Estonia (1), Finland (1), France (1), Germany (5), Hungary (1), Ireland (2), Italy

[100] TIM-Dual-Use is a web platform designed to map dual-use technologies based on Annex I of the EU regulation, as well as emerging technologies with potential dual-use applications. This tool relies on a database of three types of documents: Scopus scientific publications, patents, and EU-funded projects (CORDIS). For this research, only the last category was considered, filtering results to identify dual-use publications within EU-funded projects from 2014 onward. Official source of the tool: 'TIM Dual-Use', available at: https://knowledge4policy.ec.europa.eu/text-mining/tim-dual-use_en.

[101] European Export Control Association for Research Organisations, 'About EECARO', available at: https://eecaro.eu/about-eecaro/.

(2), the Netherlands (4), Norway (2), Romania (1), Spain (3), Sweden (1), Switzerland (1), and the United Kingdom (1).

2.2.4. Findings and discussion

This section presents and discusses the findings from the literature review, desk research, interviews, and the survey conducted in the framework of this study. It begins by outlining the typical lifecycle of an EU-funded project and mapping the stages where dual-use concerns arise. Additionally, it highlights the phases that, according to the stakeholders consulted, present more significant challenges. This is followed by an examination of the different categories of RPOs and their approaches to various phases of a research project. Finally, the key challenges in implementing dual-use R&I in EU-funded projects, along with potential pathways forward, are categorised based on recurring themes identified through the mixed-methods analysis These categories aim to provide a structured overview of the most prevalent issues encountered by stakeholders and offer insights for future improvements and areas requiring further attention.

Mapping the areas where dual use questions arise

By analysing the full lifecycle of EU-funded research projects—from inception to conclusion—and drawing on insights from the interviews conducted for this study, several key phases can be identified.

Figure 4: Simplified visual representation of the lifecycle of EU-funded research projects

Source: The author

Findings from the interviews indicate that dual-use concerns can arise at any stage of the research project lifecycle. However, some phases present more pronounced challenges and require greater attention than others, which will be discussed later, after first presenting the different phases of the research project lifecycle.

Proposal phase. During the proposal phase, researchers generally have significant freedom in designing and proposing their research. Once the proposal is conceived, structured, and detailed, it must be submitted following the EU's application procedures. At this stage, an initial ethical and security evaluation is required as part of the application process, which may prompt early identification of dual-use concerns. However, identifying potential dual-use items at this early stage is often difficult. Researchers may not yet fully anticipate the equipment, technology, or software that will be used over the multi-year course of the project. As a result, dual-use considerations may not always be a central focus at this stage, except in fields with a higher likelihood of controlled items, such as nuclear research. In such cases, broad initial assessments may be made, though the specifics often remain unclear. Additionally, some RPOs conduct screening of potential partners at this stage, which can require significant time and effort.

Grant agreement phase. Once the proposal is approved, a grant agreement must be signed. This phase triggers increased attention to compliance, as researchers and institutions must carefully review project rules, understand legal requirements, and assess the consequences of potential breaches. The awarding of project funding often marks the first significant focus on dual-use issues by researchers and RPOs.

Consortium agreement phase. Following the grant agreement, a consortium agreement is signed among participating entities. This phase is often identified as one of the most critical for dual-use concerns. When non-EU countries are involved, additional due diligence may be required, including screening of entities for sanctions, embargoes, and potential foreign interference;

negotiation of export control clauses to ensure compliance with all applicable laws; clarification of confidentiality and ethical obligations for all partners.

Project execution phase. During project execution, dual-use concerns can arise in various situations, such as storage and sharing of sensitive information; shipping of equipment and materials; hiring of foreign researchers and foreign PhD students; publication of research findings in open access. In practical terms, this is the phase where the classification of potential dual-use items is most likely to take place, and an export license should be requested if required.

For example, in an EU-funded project involving multiple participants, including those from non-EU countries, if dual-use items need to be transferred—whether as physical goods crossing borders or through intangible technology transfers—certain export control procedures must be followed. In such cases, the RPO should submit a request for a global licence (or, in some cases, a general licence) to its national authorities. This request must include: (1) end-use declaration—the stated end-use of the exported items, requiring RPO to obtain an end-use certificate from all involved RPOs; (2) control list classification—the control list item code(s), as well as the corresponding CN code(s) for physical goods; (3) exported quantity and value—the total exported quantity and value, specifying the appropriate unit of measure and currency (for intangible technology or services, only the value and currency need to be specified); (4) item description—a detailed description of the item(s) being exported; (5) trade partner information—details on the trade partner(s), which may include the end-user, consignee, third country, exporter, or third party. This information should include among other, where applicable, the partner's VAT number, national registration number, activity sector, and relationship with the economic operator. Additionally, the RPO must demonstrate the existence of an Internal Compliance Programme (ICP) in order to qualify for a global licence. Once issued, the licence is typically valid for up to two years, unless the national competent authority decides otherwise. If the licence is still required for the transfer of items within the framework of a given research project, the procedure must be repeated, including obtaining new end-use statements, to secure a renewed and valid authorisation.

A thorough understanding of export control rules and procedures is crucial—not only at the EU level but also at the national and international levels. Throughout the project lifecycle, continuous monitoring may be necessary to track the evolving nature of research. Oversight during the entire cycle of the project is essential for detecting specific dual-use concerns and identifying unforeseen developments in the research. For example, Technology Readiness Level (TRL)[102]—a widely used metric to assess technological maturity—may be low at the beginning but increase over time. As TRL advances, the level of scrutiny on information exchanges and technology transfers may also rise. This applies not only to material transfers but also to intangible aspects such as technical assistance, participation in conferences and webinars, and the hosting of researchers temporarily residing in the EU.

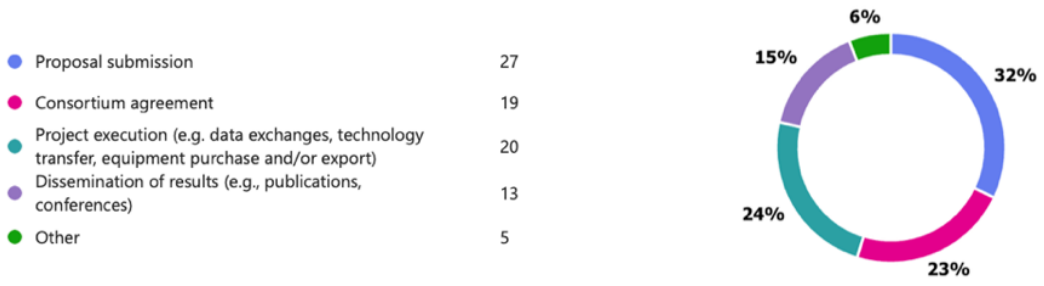
Dissemination phase. At the conclusion of the project, research findings must be disseminated, often with an open-access requirement for civil-focused EU-funded projects. Before publication, results should be screened to assess whether they contain dual-use items.

While these issues can arise at any point in the research project lifecycle, certain phases present more significant challenges and require heightened attention. The following figure highlights the project stages that survey respondents identified as particularly problematic and where they most frequently encounter dual-use concerns. It is important to note that the stages presented in the survey do not perfectly align with those outlined in the research project lifecycle in Figure 4. This discrepancy exists because the survey was launched before gathering the insights from interviews that informed the development of Figure 4. For instance, the grant agreement phase was not specifically included in the survey, yet interviews revealed it as an important moment when attention to dual-use concerns is often triggered. Additionally, the survey includes the category

[102] Under the Commission Recommendation (EU) 2021/1700, for export control purposes, research output from TRL 1 and 2 is generally considered basic scientific research. Meanwhile, the eligibility of research output from TRL 3 and 4 is assessed on a case-by-case basis. However, different interpretations may exist, such as the German approach, which considers research output from TRL 1 to 3 as basic scientific research. (See BAFA (2023), 'Manual - Export Control and Academia', p. 80.)

"Other" to capture additional stages that respondents may have considered relevant but were not explicitly listed in the survey. However, none of the respondents who selected “other” provided further information or clarification.

Figure 5: At which stage(s) of the project does the question of dual-use items arise?”



Source: Survey by the author, February 2025

The proposal submission phase was the most frequently selected, followed by the project execution phase and the consortium agreement phase when respondents were asked at which stage of the project dual-use items arise as a question.

Interviews further revealed that proposal submission for a project potentially involving dual-use items can be “time-consuming”, as it often involves partner screening, which can be particularly challenging for large consortia. In some cases, proposals may also undergo ministerial review for feedback. Additionally, application forms are not always perceived as clear and straightforward. As discussed below, perceptions of the challenges associated with this phase can vary significantly depending on the level of compliance and export control culture within a given RPO.

During project execution, administrative burdens tend to increase significantly, especially when transferring dual-use items—both tangible and intangible—to non-EU partners, with the latter often posing greater challenges. Therefore, continuous monitoring is essential to track research developments and ensure compliance with dual-use regulations.

Finally, dissemination can present a number of challenges when dual-use concerns conflict with open-access requirements. Different national authorities approach, and applicable obligations can complicate compliance with EU funding mandates.

These issues will be explored further in the following section, which discusses the key challenges faced by RPOs in implementing EU-funded projects with dual-use concerns. Before diving into the challenges, an overview is provided of how RPOs manage project implementation across these phases, derived from the comparative analysis of interviews and desk research.

RPOs’ approaches to dual-use R&I related issues

Procedures for handling research projects that may involve dual-use items vary significantly across RPOs. There is no single, standardised approach, as compliance can depend on multiple factors, including:

- the nature of the organisation or institution type (e.g., university vs. non-university);
- the internal structure (e.g., centralised vs. decentralised decision-making);
- resources and compliance culture (e.g., dedicated export control programmes vs. reliance on general legal services);
- experience with dual-use and defence research (e.g., frequent engagement vs. rare or no engagement);
- the organisation’s primary research focus (e.g., fundamental vs. applied research);

- national legal and administrative frameworks for the implementation of EU export control regulation.

Moreover, as mentioned earlier, the structured integration of compliance measures for dual-use item controls within RPOs is a relatively recent development. Some stakeholders have noted variations among research organisations, as well as between countries, in the adoption of compliance measures. One observation is that '*while some take almost no measures, other universities have established, from 2021/2022 onwards, an internal compliance program, […], have awareness campaigns in place and provide support to researchers, support staff and higher management to be compliant with the export control regimes […]*'[103].

Building on the results from desk research, complemented by interview findings, a simplified but useful framework has been developed by grouping RPOs into three broad analytical categories. Investigating and conducting a comparative analysis of the varying approaches and internal structures of RPOs seems crucial for gaining a deeper understanding of the current landscape of compliance with export control regulations in research. This analysis not only sheds light on the existing state of play but also identifies areas where improvements can be made to create a more conducive environment for compliance and successful project development.

Based on this analysis, RPOs have been here broadly grouped into three categories:

- *Highly regulated and experienced institutions*. Among these are those organisations that frequently engage with dual-use or defence-related research and tend to have a clear understanding of compliance requirements. They often have mature ICPs and well-defined, sometimes strict, procedures in place. These institutions generally allocate significant resources to dedicated staff responsible for identifying and managing the transfer of dual-use items, ensuring compliance with national and international regulations.
- *Limited or emerging awareness institutions:* Some organisations are not engaged in military research but may occasionally encounter dual-use concerns, for example in applied science, testing, and prototyping activities. These institutions may be in the process of developing compliance mechanisms, implementing an ICP, or gradually increasing awareness of export control regulations. The level of vigilance varies based on the organisation's leadership priorities and available resources.
- *Minimal or no compliance structures:* Institutions that focus primarily on basic scientific research and/or have no involvement in defence-related projects may sometimes lack dedicated compliance frameworks. In some cases, their legal structures prohibit military-related work altogether. These organisations typically rely on general legal services without specific expertise in export control, meaning that compliance procedures, if any, are minimal and reactive rather than proactive.

By categorising RPOs in this way, we can gain a clearer picture of the disparities in their way to handle dual-use research.

As a result, varying levels of awareness, practices, procedures, and compliance exist across different RPOs. This makes it challenging, if not impossible, to pinpoint a single ('correct') way in which research organisations implement EU-funded projects involving dual-use items. However, it is precisely this variability that provides valuable insights into areas where differences exist, and where attention may be required for future improvements and support.

By cross-referencing the previously discussed phases of the project lifecycle with the operational approaches of RPOs, we can better understand how these variations play out in practice.

[103] CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper', p. 37.

Table 3: Variations of RPOs approaches to dual-use research across the project lifecycle phases

Stage	Strong control and oversight	Medium or limited control and oversight	Rare or no control and oversight
Proposal submission	Support and administrative checks, including screenings.	Generally free, with possible support and administrative check including screenings, if flagged by the administration and/or researcher.	Researchers submit freely, with no support on specific dual-use issues.
Grant agreement	Careful review of the project and the agreement by compliance officers.	Reviewed by export control officers only if flagged by the administration and/or researcher.	Researchers handle it independently, with limited support in specific cases by legal department.
Consortium agreement	Thorough screening of all partners and negotiation of agreement clauses.	Possible screening of specific (potentially sensitive) partners, with or without negotiation on clauses.	No or very rare screening.
Project execution	Classification of all relevant items, notification and licence procedures for exports, technical assistance, and intra-EU transfer and strict compliance monitoring.	Attention given mostly if the project is flagged by the administration and/or researcher.	No or minimal oversight.
Oversight during the project lifecycle	Continuous monitoring of TRL evolution, with ongoing checks on information and goods exchange.	Possible oversight only if the project has been flagged as sensitive by the researcher and/or administration.	No or very rare oversight.
Dissemination of results	Strong control and mandatory pre-approval.	Review only if the project has been identified as potentially sensitive.	No or minimal review.

Source: The author

The above provides an indicative and approximate view of the compliance landscape within RPOs regarding the specific phases of EU-funded projects. The culture and practices related to dual-use controls can vary significantly depending on the factors outlined earlier. The degree of support and oversight provided to researchers can differ across the entire project lifecycle—from the inception phase, through partner screening and consortium formation, to the ongoing monitoring of transfers of goods and technology, and finally, to the compliant dissemination of results. This variability is largely driven by the institutional culture and the resources allocated to export control issues within research organisations.

In general, the more rigorous the control and oversight of projects, the higher the compliance with dual-use item regulations, resulting in a more predictable and favourable environment for researchers. It is noteworthy that “control and oversight” is not a distinct phase but rather a transversal element that applies to all stages of the project lifecycle.

Based on the data collected in this study, the first category of highly regulated and experienced institutions appears to be the least common. The majority of stakeholders interviewed belong to the second category—institutions with limited or emerging awareness. This highlights a key point of concern: European RPOs, particularly those with less established export control structures and a compliance culture, require major attention and support from European and national authorities.

Their internal structures, resources, and expertise may sometimes fall short compared to e.g., industry counterparts, where centralised resources can be focused on detecting dual-use items and ensuring compliance with export control regulations. In contrast, non-profit research

organisations may often lack the specialised human resources, such as lawyers with expertise in sanctions, export control officers, and similar professionals.

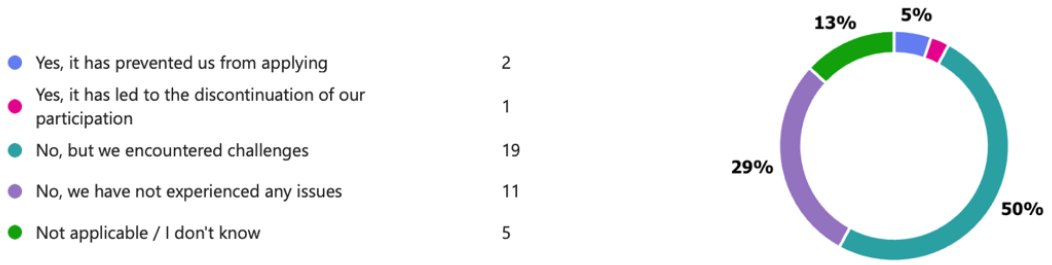
Regardless of the category, and despite varying levels of expertise and resources allocated to dual-use item trade controls, significant challenges and grey areas remain in implementing export controls in research projects—particularly in the context of EU-funded projects. Even where well-established procedures are in place, questions around the practical application of these controls persist. These range from the early identification of sensitive cases amid the vast number of EU-funded project proposals to the effectiveness of screening mechanisms, oversight during project execution, and ensuring compliance in the dissemination of results.

Challenges in implementing EU-funded dual-use R&I research

The stakeholders interviewed in this study expressed openness and strong interest in pursuing dual-use research, recognising it as an important area of investigation that offers significant opportunities for technological advancement. Given its potential, stakeholders believe that dual-use research should continue to be pursued, ideally under more favourable conditions.

At present, while the majority of stakeholders consulted in this study acknowledged facing challenges in implementing dual-use research, these challenges have not been severe enough to deter them from applying for or continuing participation in EU-funded projects.

Figure 6: Has the involvement of dual-use items in an EU-funded project ever prevented you or your organisation from applying or continuing participation?



Source: Survey by the author, February 2025

According to survey results, only two respondents (5%) indicated that the involvement of dual-use items in EU-funded research projects had prevented them from participating, and only one (3%) reported that it led to their discontinuation from a project. A follow-up interview regarding the latter case revealed that the decision to withdraw stemmed from concerns over a specific partner's end-use of shared information and technology. Due to evolving geopolitical developments, this partner was perceived as posing a heightened risk in terms of potential misuse of technology and research results.

The report has identified several key challenges that stakeholders face when implementing EU-funded research projects involving dual-use items. These challenges range from broad, overarching issues to specific obstacles that create tension, uncertainty, and administrative complexity. The major recurring challenges highlighted in this report include:

- Navigating collaboration with project partners;
- Gaps in the application phase, including limited focus on dual-use concerns and lack of detailed guidance;
- Managing export license applications;
- Challenges in classifying of dual-use items;
- Complying with open-access publication requirements;

- Essential resources for effective compliance efforts.

Navigating collaboration with project partners

When engaging in research projects in sensitive areas that may potentially involve dual-use items, particular attention must be paid to the selection of partners. It is crucial to know the entities with which one is working, not only for compliance with export controls but also for ethics and other legal considerations. As such, a screening process of potential partners is generally conducted by RPOs, particularly by their administrative staff, who possess the necessary expertise regarding embargos and other regulations. This process generally occurs either during the proposal development phase, during the formalisation of agreements, or at both stages.

However, this screening process requires significant human and financial resources and can be "time-consuming", especially in large consortia, according to most stakeholders. This makes partner screening a critical challenge for many RPOs. Additionally, the need to navigate complex and diverse sanctions regimes—including those from the EU and the US[104]—adds to the complexity. The tools available for conducting these checks, as well as the overall investment in screening practices, vary significantly across RPOs. Consequently, the level of diligence in assessing entities involved in EU-funded projects with potential strategic importance is inconsistent, leading to uneven risk mitigation efforts.

Some stakeholders noted that their organisations conduct minimal screening, assuming that if the EU has accepted an entity, it must be compliant with relevant regulations. Conversely, others reported taking responsibility for screening, arguing that the EU does not conduct sufficient checks. Moreover, stakeholders noted that most of the times they lack access to the necessary information to perform a thorough investigation, such as data on ultimate business owners or intelligence information about the entities involved. This lack of access can vary across organisations and countries.

Furthermore, the screening process made by participants in EU funded projects may be inconsistent, depending on national legislations and policies of the countries involved in the EU project, particularly those from associated countries that may have different export control rules and sanctions lists. Yet, as the 2021 Recommendation highlights, '*the export screening process is at the very heart of the organisation's internal compliance measures'*, underscoring its importance in ensuring compliance[105].

One of the most critical moments in establishing a consortium is negotiating and signing the consortium agreement. RPOs that are well-versed in dual-use issues and export control rules may negotiate legal clauses specifically addressing compliance with export control regulations. These agreements may sometimes require partners to complete questionnaires on topics such as US technology involvement or the end-use of transferred goods. Some RPOs draft their own agreements or use models, such as the DESCA Model Consortium Agreement[106]. However, interviews revealed that not all RPOs are familiar with this model, and there is no standardised or referenced EU template for consortium agreements within the project implementation framework, which could suggest the inclusion of such clauses, or other specific ones, such as a no-Russia clause.

Insights gathered from stakeholders indicate that varying levels of awareness of dual-use item transfer issues can lead to significant challenges and tensions in project implementation. For example, RPOs with a low level of compliance may find the practices of more compliant partners

[104] Despite the EU's 'blocking statute' (Council Regulation (EC) No 2271/96 of 22 November 1996), which prohibits compliance with laws passed by another country that have extraterritorial impacts, there are known examples where universities of science and technology in Europe, as well as other research organisations, have complied with the extraterritorial scope of these sanctions, particularly concerning the re-export of US-originating software and technology. Cf. CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper', p. 20.

[105] Commission Recommendation (EU) 2021/1700, p. 29.

[106] This Model Consortium Agreement for EU research projects was developed collaboratively by a group of eight research organisations. DESCA website: https://www.desca-agreement.eu/desca-model-consortium-agreement/.

to be obstructive, as they may introduce additional administrative burdens and could slow down project processes, especially when partners require a significant amount of documentation or information to ensure compliance.

Gaps in the application phase, including limited focus on dual-use concerns and lack of detailed guidance

In the Horizon Europe application form, dual-use is mentioned only once, within the "Declarations" section. Applicants are required to tick a box confirming that their proposal focuses exclusively on civil applications. Additionally, if the project involves dual-use items as defined in Regulation 2021/821, they must acknowledge their obligation to comply with the relevant regulatory framework. This remains the sole explicit reference to export control for dual-use items within the application process.

Figure 7: Extract from Horizon Europe standard application form, section "Declarations", p. 3

7)	We declare that the proposal has an exclusive focus on civil applications (activities intended to be used in military application or aiming to serve military purposes cannot be funded). If the project involves dual-use items in the sense of Regulation 2021/821, or other items for which authorisation is required, we confirm that we will comply with the applicable regulatory framework (e.g. obtain export/import licences before these items are used).	☐

Source: Horizon Europe standard application.

The majority of RPOs involved in the inquiry of this study stated that simply ticking this box is insufficient. They find it challenging that, at this stage, there is minimal effort to raise awareness of the issue, provide additional information, or offer clarification on export control regulations. Researchers risk selecting the option without a full understanding of its implications. There is a lack of detailed guidance at this point, and no clear instructions on how to address potential dual-use concerns. As one stakeholder noted, '*even if the box is ticked, there is no follow-up or support to determine what the project beneficiaries need to do.'*

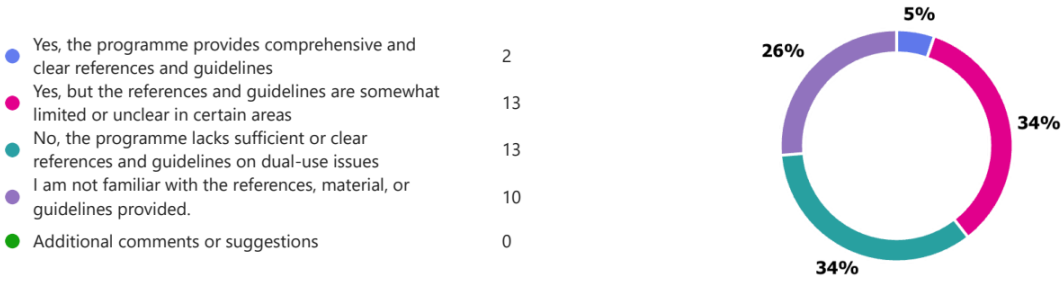
Researchers may struggle to navigate the extensive legal and regulatory texts, or the ICP recommendations, in an attempt to understand what constitutes dual-use and the potential implications for their projects. Stakeholders also observed that the term dual-use is sometimes misinterpreted, with vague definitions leading to overly broad interpretations—such as the notion that everything could be considered dual-use. There is a need for clearer explanations of how the term relates to the annexes of the regulation and its specific meaning under EU law. It should be made explicit that not all research involves dual-use items, and researchers should not be discouraged or alarmed unnecessarily.

Additionally, non-EU countries may have different interpretations of the rules or rely on their own national regulations, which can sometimes diverge from EU standards, particularly regarding controlled items (e.g., emerging technologies, as well as open access publications, are not uniformly controlled across all countries). This lack of alignment could negatively impact project implementation, as stakeholders warned that '*not everyone is on the same page',* ultimately leading to tensions. RPOs with a higher level of awareness and compliance expressed frustration over working with partners who do not share the same level of understanding or attention to export control issues.

Moreover, stakeholders perceived that legal and ethical considerations were sometimes conflated, with an unclear distinction between the two. They also noted that, while numerous questions are asked during the application process, there is a lack of proportionate attention and instructions given about export control requirements for dual-use items in research projects.

According to survey results, there is no full and widespread satisfaction with the availability of references, informational materials, and guidelines on how to manage dual-use concerns within projects.

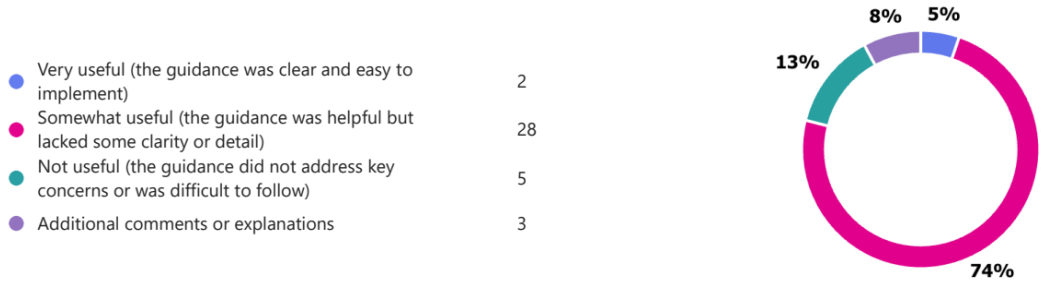
Figure 8: Do you think the current programme, Horizon Europe, provides sufficient references, informative material and/or guidelines on how to deal with dual-use issues within the project?



Source: Survey by the author, February 2025

Regarding other guidance provided, such as the Commission Recommendation (EU) 2021/1700 of 15 September 2021 on ICP, stakeholder feedback varied and revealed more widespread satisfaction with it.

Figure 9: Stakeholders' responses to the survey question: Have you found past and current guidance on research involving dual-use items useful (e.g., Commission Recommendation (EU) 2021/1700 of 15 September 2021 on Internal Compliance Programmes)?



Source: Survey by the author, February 2025

The majority of respondents considered the guidance somewhat useful, expressing concerns that it lacked clarity in certain areas. Insights from interviews further highlight that while these recommendations are particularly valuable for establishing or implementing an ICP—primarily benefiting administrative and compliance officers—they are less accessible for researchers seeking a straightforward understanding of export control in the context of Horizon Europe-funded projects.

Managing export license applications

RPOs may encounter significant challenges when applying for export licenses, particularly in large consortia or when classified dual-use items must cross multiple borders for activities such as testing. This remains the case even when utilising the licensing and facilitation mechanisms provided by the EU dual-use Regulation. The classification process must be completed before submitting a license application or requesting clarification from the competent authority. However, timelines for discussions with authorities—and especially for obtaining licenses—can vary widely across countries. This is further complicated by differing national interpretations of export controls, particularly concerning intangible technology transfer related issues.

Beyond the procedural delays and inconsistencies among national authorities, additional difficulties arise when an end-use certificate is required by one or more consortium members as

part of internal procedures or license applications[107]. This can create tensions due to differing understandings of the applicable regulations.

Another challenge is that, as some stakeholders noted '*the types of licenses foreseen by the EU dual-use Regulation do not align with the requirements of EU-funded projects.'* For instance, "the collection of multiple end-use certificates by the Consortium members, or the required details in the license applications (value and origin of the technology, country of destination and end use) clearly do not fit with the needs of the big consortia participating in such funded projects"[108].

Further obstacles include difficulties in accessing clear guidance on specific export control issues in research, such as the procedures/controls for hiring non-EU PhD students. Stakeholders also highlight the absence of a centralised EU-level contact point for inquiries on these matters, adding to the complexity of project implementation.

Finally, in specific cases, such as research involving nuclear-related items or those covered under Annex IV of the EU Dual-Use Regulation, intra-EU transfers may also require careful oversight and specific procedures, resulting in additional administrative burdens. Even for Annex I items, intra-EU transfers can necessitate classification and related compliance efforts, which can further complicate the execution of research projects[109].

Challenges in classifying of dual-use items

Classification remains one of the most significant challenges that RPOs face when implementing projects involving or potentially involving dual-use items. Determining whether a technology falls under EU export control regulations involves a complex classification process based on the specifications in Annex I of the EU Dual-Use Regulation, regardless of its stated, suspected, or potential military use[110]. Additional complexities can arise in the case of catch-all controls.

Figure 10: How challenging has it been for you to determine whether a research project involves dual-use items?

Source: Survey by the author, February 2025

The majority of survey respondents (97%) report facing "some challenges" or "significant challenges" in determining whether a research project involves dual-use items. No respondents reported facing no challenges at all.

Identifying and classifying an item against the EU list and regulations requires a thorough understanding of the framework and the ability to navigate through hundreds of pages of technical specifications. It also demands a certain level of control from RPOs over proposal submissions and ongoing project oversight, as well as the expertise to determine for example whether an item

[107] According to Article 12(4) of Regulation (EU) 2021/821, the issuance of an export license is conditional upon the submission of an end-use certificate.
[108] European Export Control Association for Research Organisations (2024), 'Feedback on the White Paper on options for enhancing support for research and development involving technologies with dual-use potential', p. 3.
[109] Article 11.9 of Regulation (EU) 2021/821 requires that 'the relevant commercial documents relating to intra-Union transfers of dual-use items listed in Annex I shall indicate clearly that those items are subject to controls if exported from the customs territory of the Union. Such documents include, in particular, any sales contract, order confirmation, invoice or dispatch note'.
[110] European Export Control Association for Research Organisations (2024), 'Feedback on the White Paper on options for enhancing support for research and development involving technologies with dual-use potential', p. 3.

could be an emerging technology subject to controls. Ideally, researchers should handle the classification themselves, but as stakeholders have noted, "*it is not always easy to get them there.*"

In institutions with an export control officer and dedicated staff, the officer typically supports the researcher in this task, ensuring that the researcher performs the classification correctly, provided that a dual-use item has been identified in the research.

Figure 11: How challenging has it been for you to classify dual-use items in your project (e.g., determining the precise classification number according to the annexes of the EU Dual-Use Regulation 2021/821)?

Source: Survey by the author, February 2025

The complexity of navigating technical parameters to determine whether an item is subject to controls, understanding the laws regulating them, and the lack of clear guidance and training on classification processes present some challenges and significant challenges in 89% of the survey respondents. Many stakeholders have emphasised that a few pages of straightforward instructions on how to approach classification would be beneficial. Additionally, the lack of incentives for researchers to engage in export control processes further complicates matters. Some RPOs can develop and provide education and internal training materials, depending on the institution's commitment to compliance with export control rules.

Interviewees explained that significant complications arise when projects involve US-origin technology, as these require additional classification and compliance procedures. Moreover, regardless of an institution's level of compliance or the resources available, challenges remain when it comes to classifying emerging technologies. Researchers, organisations, and authorities often have limited experience in this area, making it difficult to identify technologies that may not yet exist or are just being developed but still fall under dual-use regulations. This lack of familiarity makes the classification of emerging technologies particularly challenging for everyone involved.

Nevertheless, classification is a critical part of compliance. It plays an important role when transferring dual-use items out of the EU, triggering license requests, and for intra-EU transfers, particularly for Annex IV items requiring licenses, or when providing specific details for intra-EU transfers of Annex I items. Finally, tensions can also arise within consortia when there is no agreement or a shared understanding regarding the classification of certain items.

Complying with open-access publication requirements

Stakeholders often highlight a tension between the EU's requirement to disseminate the results of civil-focused research projects in open access and the constraints imposed by export control regulations on dual-use items. This tension is exacerbated by the varying levels of compliance by RPOs with export control rules, as well as the differing experience and approach of national authorities with dual-use items—particularly in the context of intangible technology transfer and publications. Many export control licensing systems are primarily designed around the transfer of physical goods, such as customs verification and procedures, making the situation even more complex. In fact, it appears that most countries lack a system to process export control applications for publications, as the process typically requires the specification of a particular end-user, end-use and other information (e.g., the value). For example, Germany allows exporters to submit a 'general inquiry' regarding publications in the system, which is processed, but not as a formal license application. In contrast, the Netherlands uses the global licensing procedure for controlled technology exports to more than one country.

Some EU third countries, instead, such as the UK, require an export license before a research publication can be sent for peer review. In this process, the end-user—the peer reviewer—is clearly identified, and only after the review is completed and the research is officially published does the license requirement lapse[111].This creates a complex scenario where RPOs, in the midst of a transition or consolidation phase in their control systems, face considerable uncertainty. Many organisations seek clarification on the interpretation and implementation of export control rules; however, national competent authorities seem to struggle to provide consistent support, with response times varying considerably. These authorities, while often well-versed in industrial applications and physical goods controls, may have limited expertise in handling issues like intangible technology transfers or export control in research contexts (e.g., the storage of information in specific clouds or who the end-user of a publication is). This gap in knowledge leads to a situation of uncertainty, where stakeholders actively seek guidance but do not always receive a definitive answer.

The approach taken by different countries and authorities—including within EU countries—towards open access publication can vary widely. Some authorities may discourage the publication of research involving dual-use items, while others may be more open to discussion and identifying mitigating actions. In contrast, some may impose almost no restrictions at all. These differing approaches can result in an uneven playing field in research implementation, where the ability to publish research could depend on the country in which the research is being conducted.

It is noteworthy that no instances of research involving dual-use items requiring a publication license were found in the framework of this study. Furthermore, as others have pointed out, open access publications are, at present, only minimally affected by export control and other knowledge security measures, while issues like intellectual property and trade secrets appear to have a more significant impact on research[112].

A recurring theme among stakeholders is that many of the questions surrounding export controls and open access publications are hypothetical. For instance, researchers may ask, '*What should we do if our results involve or result in dual-use items, but our competent authorities discourage us from publishing, and the EU-funded programme requires dissemination in open access?*' Additionally, varying levels of compliance among RPOs can lead to a situation where researchers may choose to publish with an RPO that applies fewer export control rules, thereby bypassing stricter compliance measures. This can ultimately create competitive disadvantages.

In times of uncertainty, researchers may be motivated to focus their work on more basic scientific investigations in order to take advantage of exemptions from controls offered by EU regulations. However, as some stakeholders have expressed, '*publications and presentations rarely meet the control thresholds in their entirety, but it reflects a significant future barrier for (open) scientific processes*'[113]. Therefore, the interplay between open access requirements and export control regulations may be viewed as a growing concern, one that may pose a challenge to the future of scientific research and dissemination.

Essential resources for effective compliance efforts

Detecting and tracking the lifecycle of research projects with sensitive components is no easy task. As illustrated in the table 3 above, which outlines the different approaches of RPOs throughout the various project phases, there is a considerable range in how the issue is handled depending on the level of awareness and compliance, which is intertwined with the resources allocated. In some cases, there is a systematic screening and detection of sensitive cases, while in others, these issues are only identified when communicated by other administrative departments within the RPO or, in some instances, identified by the researcher themselves.

[111] UK Government (2021). 'Export controls applying to academic research', Guidance.
[112] CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper', p. 47.
[113] *ibidem*, p. 8.

Researchers are constantly pushing the boundaries of science and technology, making continuous discoveries and progress. Allocating adequate human resources to support this task is crucial for helping researchers understand and comply with applicable regulations. Additionally, raising awareness among researchers by introducing them to the topic through education and training and explaining necessary compliance practices is essential to fostering a proactive approach to dual-use concerns. However, not all RPOs seem to allocate sufficient resources to this. As one interviewee noted, '*there is no way to have a dedicated control officer following the entire cycle of a research project*.' Despite this challenge, someone should be monitoring the research as it evolves, with the primary responsibility falling on the researcher. In some cases, RPOs hire external consultants to navigate export control regulations, including with regard to US legislation and compliance. While external support can be helpful, having skilled in-house resources with expertise in export control regulations remains crucial, but it remains still a significant challenge. The complexity of issues like technology classification and the dynamic nature of export controls further highlights the need for skilled personnel within research organisations[114]. Lastly, beyond human resources, which also require financial investment, allocating funds to tools, compliance software, and other infrastructure may be crucial. For example, software solutions can help exporters automate international trade processes, manage partners and compliance-related documents, minimise the time spent on screening, and ensure their company stays up to date with ongoing revisions and amendments to international legal requirements. However, these solutions can be very expensive and represent a significant investment compared to the available resources or the budgets allocated by many RPOs for compliance. Yet, this investment can significantly enhance compliance efforts and help RPOs better manage the challenges associated with dual-use research.

Box 2: Case study on export control challenges in a Horizon Europe consortium project

In this example, an RPO based in EU Country X is working on a Horizon Europe-funded project involving multiple partners across several countries. The project focuses on developing advanced technologies and includes the exchange of sensitive materials, such as those classified under Annex IV of the EU Dual-Use Regulation. All partners have licenses in place for the other countries, including the RPO in country X, where the license is valid for three years.

Challenges faced

→ *Uncertainty in material exchange quantities and parties involved:* The project is still in its early stages, and the exact quantities and identities of the materials being exchanged are not yet clear. This makes it difficult for consortium members to plan for the required export control licenses.

→ *License validity mismatch with project duration*: The export control licenses required for the exchange of Annex IV materials are valid for only 3 years in Country X, while the project itself spans 4 years. This means that in the fourth year, the process must be repeated. Redoing the process involves collecting and obtaining updated end-use certificates from all participants, determining the routes and parties involved in the material exchange, potentially reevaluating the research's compliance with regulations, and waiting for several months to get the licenses in order again. This process can be significantly slower in some countries compared to others. The time-consuming nature of these processes can create logistical burdens and risks delays, especially if unforeseen issues arise during the license renewal.

→ *End-use certificates and compliance coordination:* As part of the export control process, the consortium must collect end-use certificates for the materials being transferred. These certificates, required by the competent authorities, confirm the intended use of the materials and must be obtained from each partner. Coordination among multiple parties can be challenging, and delays in obtaining these certificates can affect the project's timeline.

→ *Open access requirement conflicts with applicable rules:* Another significant challenge arises regarding the dissemination of results through open access. While the majority of the research results can be published freely, some deliverables contain dual-use technologies that fall under restrictions.

[114] European Export Control Association for Research Organisations (2024), 'Feedback on the White Paper on options for enhancing support for research and development involving technologies with dual-use potential', p. 2.

Therefore, the project consortium is required to obtain a license to make these deliverables publicly available, but it will theoretically be unable to do so in some countries due to the Russia sanctions.

Source: Interview by the author, February 2025.

Potential measures and strategies for improvement suggested by stakeholders

As noted earlier, the challenges faced in R&I dual-use projects funded by the EU are not unique to the EU framework but often arise more broadly in research environments. This section highlights key areas of concern, practical suggestions, and ideas from stakeholders—collected through interviews, surveys and desk research—aiming at improving the handling of dual-use items in EU-funded research projects. The chapter offers insights based on practitioners' experiences with dual-use compliance in these projects.

The input gathered identifies potential measures and strategies for improving the implementation of dual-use projects under current and future EU programmes:

- Greater focus on dual-use concerns during the application phase, with enhanced guidance and support for stakeholders, including dedicated points of contact;
- A licensing process better suited to Horizon Europe projects, including an EU-wide license system and a more uniform approach by national authorities to handling license requests and information (e.g., response timeframes);
- Increased support for the capacity of RPOs;
- A dual-use flagging mechanism;
- Education and training for researchers and RPOs, and awareness campaigns by national and European authorities.

Addressing gaps in the application phase, and the need for more guidance and support

One of the most frequent requests from stakeholders is for additional guidance, instructions, and clarifications. This need was consistently emphasised in interviews, surveys, and feedback from recent consultations on export control and research. Providing more resources in this area could help address several challenges and enhance the management of dual-use issues in EU-funded R&I projects. Clearer guidance could bring multiple benefits.

First, it would raise awareness and ensure a level playing field. It is essential for all project participants to understand the implications of dual-use item transfers from the outset. Easily accessible materials—such as leaflets explaining export controls, video tutorials, simple guides on identifying and managing dual-use items, and visual aids illustrating Annex categories—can significantly enhance awareness and compliance. This includes aspects such as classification, understanding TRLs, and applying exemptions for basic scientific research or publicly available information. Additionally, integrating dedicated sections and requirements within the project application process, beyond merely "ticking a box", would ensure that all participants operate with the same foundational understanding. This would benefit not only legal and administrative teams but also researchers, promoting consistency across EU-funded projects.

Second, clearer guidance would help reduce uncertainty. Providing upfront explanations of key concepts—such as the definitions of “dual-use items” and “technology” under EU regulations—would eliminate ambiguity and offer researchers practical support. Clarifying potential consequences and compliance steps would prevent delays caused by the need for additional clarifications from national authorities.

Third, it would help alleviate concerns and address frustrations. Researchers and export control officers often experience difficulties due to a lack of readily available guidance or clear interpretations of regulations. Providing additional resources—such as FAQs and detailed explanations—could clarify expectations, particularly regarding open-access publication

requirements. This would support researchers in identifying dual-use research, what steps to take when encountering dual-use issues, and how to navigate public dissemination requirements.

Moreover, clearer guidelines would help reduce tensions in consortium agreements by ensuring that all parties have a better understanding of the applicable rules, thereby minimising misunderstandings and inconsistencies. Increased awareness and knowledge of export control regulations would create a more informed environment, fostering smoother collaboration among partners. As an additional tool, introducing and referencing an EU template model for consortium agreements—including standardised clauses and provisions related to export controls—could further support researchers and institutions in navigating these requirements within a secure and compliant framework.

As highlighted by EECARO in their input to the white paper on export control, '*the key for operational success in implementing export control laws in a research context is clear guidelines in addition to clear regulatory requirements*'[115]. This need for guidance was further reinforced in consultations on R&D dual-use options[116]. In addition to supporting materials, stakeholders emphasised the necessity of a point of contact at the EU level to address questions and concerns regarding the involvement of dual-use items in EU-funded research projects. Several organisations and associations have echoed this call in their position papers, advocating for the creation of a dedicated "help desk" to assist researchers and universities in navigating complex regulations[117]. Such a support structure would help clarify how authorities interpret and implement the regulations (including how thresholds are determined) while ensuring that research remains as open as possible.

Overall, providing more guidance could help address multiple challenges, such as improving classification processes, fostering collaboration among project partners, and reducing potential tensions caused by differing interpretations of rules or requirements. Furthermore, clearer guidance could help researchers better understand open access requirements and how they relate to dual-use research. With stronger support, researchers and RPO administrations would be better equipped to navigate regulatory challenges, ensuring more favourable conditions for advancing such projects.

Making the licensing process fit the Horizon Europe projects' context

Insights from stakeholders, as well as the real-case example referenced earlier, highlight how uncertainties surrounding material exchange, mismatched licensing durations, and the need for multiple end-use certificates can create a complex and time-consuming compliance environment. Additionally, the current licensing systems for technology transfer, particularly in relation to publications, are often ill-suited for research projects. A coordinated effort between the European Commission and EU Member States could greatly improve this situation. Stakeholders interviewed, along with others who contributed to consultations, have suggested the introduction of an EU general licence tailored specifically for Horizon projects. Such a licence, granted alongside project approval, could significantly reduce administrative burdens and streamline compliance procedures.

Another key suggestion is for national competent authorities to adopt a more consistent approach to processing responses, providing information, and clarifying export control matters, particularly within the context of EU-funded projects. One of the main concerns raised by stakeholders is the great variability in response times from national authorities, which can disrupt project timelines. This is a risk that stakeholders would like to see minimised. Therefore, reducing these inconsistencies would be a significant improvement.

[115] European Export Control Association for Research Organisations (2024), 'Feedback on the White Paper on Export Controls', p. 1.
[116] See for example: EARTO (2024), 'EARTO Answer to EC Consultation on Technologies with Dual-use Potential', p. 2.
[117] CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper', p. 49.

Providing more support to the capacity of RPOs

Stakeholders have also proposed that the EU consider including a dedicated work package focused on export control compliance for sensitive projects, along with additional support to facilitate effective implementation. Allowing costs related to engaging in-house or external legal advisors with expertise in export control regulations to be eligible for funding would be particularly beneficial for projects with significant regulatory complexities.

Introducing a dual-use flagging mechanism

A key overarching support measure that stakeholders believe could enhance the implementation of projects potentially involving dual-use items throughout their lifecycle is a flagging or labelling system. This system would involve evaluating and labelling certain calls—particularly those with civil/military synergies and potential dual-use concerns—at an early stage. Stakeholders see this as a transparency measure from the EU, providing early indications of the procedures and compliance requirements that might be necessary for certain projects. Increasing awareness of dual-use implications should extend not only to project coordinators but to all beneficiaries. The majority of stakeholders interviewed believe that such a system would create a more favourable environment for awareness and compliance rather than discourage participation. Many researchers are willing and interested in conducting dual-use research, and having clear expectations from the outset would provide significant support, guiding both researchers and administrative teams through the necessary procedures for EU-funded R&I projects. Furthermore, for particularly sensitive calls, imposing limitations on collaborations with specific countries or entities could be beneficial, reducing the likelihood of licence denials based on end-use concerns.

A labelling mechanism could assist RPOs and compliance officers in better identifying sensitive projects that require closer oversight. Given the high volume of EU-funded projects submitted by researchers across various fields, systematically screening all projects can be challenging for many RPOs—particularly for those with fewer resources. Some RPOs only monitor dual-use research when flagged internally by researchers or administrative units (see Figure 5), making an EU-level flagging system a useful tool for internal organisation and compliance. Additionally, such a mechanism could help organisations estimate and allocate resources for compliance monitoring early in the project lifecycle.

Another advantage of a flagging system is that it would allow for greater attention and guidance from authorities for flagged cases. More specific instructions and clearly stated EU expectations regarding partner screening and compliance with economic and knowledge security policies could also be beneficial. This pre-screening process could make it feasible to establish a dedicated help desk for high-priority cases, where researchers and project implementers could receive timely answers to concerns, including those related to publications.

Such a mechanism would also support organisations and researchers in forming consortia by providing guidance on how to manage partnerships. Beyond general guidance during the screening phase, specific assistance could be offered in drafting adaptable export control legal clauses or compliance agreements, particularly in light of geopolitical uncertainties. For example, a standardised template could be developed and suggested to address key compliance issues, e.g. allowing for the inclusion of clauses such as "no-Russia" provisions during periods of heightened geopolitical tension.

Overall, introducing a flagging mechanism for research involving dual-use items—particularly those with civil/military synergies—could enhance support structures and ensure more effective project oversight. This would help beneficiaries comply with export control regulations while minimising administrative burdens and uncertainties. Open communication with beneficiaries would be crucial in ensuring compliance and the smooth functioning of EU-funded projects. Additionally, such a mechanism could help applicants identify potential synergies between civil and defence research, making the process more transparent and manageable.

Education and training for researchers and RPOs, and awareness campaigns by national and European authorities.

Last but certainly not least, education and training on dual-use concerns in research—particularly in the context of EU-funded projects with an exclusive civil focus—play a crucial role. National and European authorities could actively engage in awareness campaigns to inform relevant stakeholders about these issues.

As seen above, throughout the lifecycle of dual-use projects and across the various actors involved at different stages, researchers and administrative staff share key responsibilities. On one hand, researchers are the ones most familiar with their projects, the technologies involved, and their specific characteristics, making them best positioned to identify and classify potential dual-use items. On the other hand, when it comes to aspects such as partner screening, license requests, and other procedural compliance matters, RPOs and their administrative staff, including compliance officers, are generally better equipped to ensure adherence to all applicable laws.

Therefore, training, education, and awareness campaigns should be tailored to these two key stakeholder groups—researchers and administrative staff—in the implementation of EU-funded dual-use projects with a civil focus. Strengthening researchers' understanding of dual-use implications from the outset, or recognising their potential emergence later in the process, would make them more vigilant and proactive in informing the relevant administrative staff. This, in turn, would reinforce the entire compliance chain.

On their end, administrative staff would benefit from training and education provided by national and European authorities, equipping them with a deeper understanding of export controls in research, the challenges related to ITT, and best practices for managing publications, large consortia, and other relevant compliance matters. By fostering knowledge and awareness at both levels, these initiatives would ultimately enhance compliance and mitigate risks associated with dual-use research.

2.3. SMEs, start-ups and scale-ups

2.3.1. Introduction

Small and medium-sized enterprises (SMEs) play a crucial role in driving innovation within the European Union (EU). Their contributions, including manufacturing and services, drive disruptive or incremental innovations and enhance value chains. Within the group of SMEs, start-ups introduce groundbreaking innovations, often exploring uncharted territories in technology and services. Their agility allows them to adapt swiftly to market demands and emerging trends, positioning them as key players in addressing societal challenges through innovative solutions. As these start-ups may evolve into scale-ups, they amplify their impact by expanding operations, entering new (cross-border) markets, and attracting more investments. This growth trajectory not only boosts the EU's competitiveness but also serves as a catalyst for regional development and economic diversification.

SMEs are implicated and impacted by the political concept of Open Strategic Autonomy that aims to enhance the EU's capacity to make independent decisions and reduce reliance on external entities, particularly in critical sectors. This approach seeks to balance openness to international collaboration with the need to protect and promote the EU's strategic interests[118]. In pursuing and maximising technological sovereignty[119], the EU faces known major obstacles, including the fragmentation of the European market, dependency on non-European technologies and supply chains, regulatory fragmentation, complexity and overreach, and diverse or conflicting Member

[118] Sirtori et al. (2024), *SMEs and Open Strategic Autonomy*.
[119] Ramahandry et al. (2021), *Key enabling technologies for Europe's technological sovereignty*.

State interest. Technological sovereignty and strategic autonomy are no interchangeable terms but contain some overlapping concerns and objectives[120].

The EU's search for finding the right balance between resilience, competitiveness and security is closely intertwined with its evolving research policies and narratives, which increasingly recognise the importance of dual-use research in enhancing both civil and defence capabilities amidst changing geopolitical dynamics and geostrategic shifts. To this end, European research policies are progressively focusing on the transition from applied research to the scale-up phase, and on exploiting the civil and defence capacity of research results. This trend is partly linked to dual-use research of concern, research security and economic security for dual-use technologies and dual-use export controls for national security, terrorism and human rights considerations.

SMEs, scale-ups and start-ups are key contributors to unlocking the potential of dual-use R&I. This part delves into the opportunities and challenges faced by these companies in the practical implementation of dual-use R&I, in particular in relation to compliance with export control. The scope is focused on existing practices in relation to R&I projects funded in the EU. It firstly takes a closer look at the role of SMEs, start-ups and scale-ups in the innovation ecosystem of the EU. It then turns to the export control awareness and implementation challenges of SMEs, start-ups and scale-ups in the EU's innovation ecosystem, with a particular focus on Horizon Europe and European Defence Fund. It concludes with opportunities to increase awareness on the relevance of the export control framework in R&I and for project participants, in particular SMEs, start-ups and scale-ups.

2.3.2. Role of SMEs, start-ups and scale-ups in the innovation ecosystem of the EU

In the EU, the indicators 'staff headcount', 'turnover' or 'balance sheet' are used to delineate the category of SMEs and its subcategories from other companies[121]. In line with the European Startup Scoreboard, start-ups are considered in this chapter as a sub-category of SMEs. Scale-ups may or may not be captured by the definition of SMEs as they expand in terms of employment and growth[122]. In this chapter, therefore the term 'SMEs, including start-ups and relevant scale-ups' will be used. The analysis and its conclusions in the ensuing sections will be applicable for the three types of enterprises, unless stated otherwise.

SMEs, including startups and relevant scale-ups, make up 99% of EU businesses[123]. They account for 98% of exporting enterprises in the EU on average in the period 2017 to 2022. While the share in number of exporting SMEs varies little among EU Member States, there is more variation in their share for their value of exports. On average in the EU, the SME share in value of exports is 37%[124].

About 1 out of 4 SMEs in the EU with at least 10 employees are R&I practitioners and carry out research and development activities[125]. Translating lab-scale innovation into a scalable, cost-effective product is complex. Early-stage innovations often require substantial additional investment beyond initial research grants. Despite significant investments in R&I, many promising innovations fail to transition from the laboratory to the marketplace as they enter the "valley of death"[126].

---

[120] Beaucillon and Poli (2023), 'Special Focus on EU Strategic Autonomy and Technological Sovereignty: An Introduction'.
[121] Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.
[122] Vandresse et al. (2023), *European startup scoreboard – Feasibility study.*
[123] European Commission, SME definition, available at: https://single-market-economy.ec.europa.eu/smes/sme-fundamentals/sme-definition_en
[124] Eurostat (2025), 'International trade in goods by enterprise size'.
[125] Eurostat (2024), 'Enterprises with research and development (R&D) activities during 2018 and 2020 by NACE Rev. 2 activity and size class'.
[126] Fiott (2019), 'The Valley of Death: Managing risk and resources'.

The positioning and significance of SMEs, including startups and relevant scale-ups, within the value chains of established industries and growing markets vary greatly. The challenges faced by both larger companies and SMEs, including startups and relevant scale-ups, include obstacles to operate seamlessly across borders, to benefit from fair competition, and to thrive in a lean regulatory environment, are well documented[127]. Numerous policy initiatives aim to enhance their positions within these value chains. Various funding programmes and initiatives, including a dedicated SME Relief Package, have been developed by the European Commission to safeguard and promote the prosperity of SMEs[128]. At the time of writing, the Commission is developing a Startup and Scaleup Strategy with foreseen adoption in mid-2025, in line with the Mission Letter for the Commissioner for Startups, Research and Innovation from the President of the European Commission[129].

2.3.3. Challenges for SMEs, including start-ups and relevant scale-ups, to participate in EU funding programmes

The Framework Programme for Research and Innovation "Horizon Europe" and the European Defence Fund (EDF) are crucial pillars of the European innovation system, each playing a distinct but complementary role in driving technological advancements, competitiveness, and strategic autonomy in Europe. Box 3 gives some key observations about the role SMEs play in Horizon Europe, whereas Box 4 focuses on the importance of the EDF for SMEs engaging in defence innovations.

Box 3: Role of SMEs in Horizon Europe

The report 'SME participation in Horizon Europe Key figures (and key issues) in the first three years'[130] contains relevant information about the role of SMEs[131] in Horizon Europe funding. Below is a summary of some key observations:

- SMEs received about 20% of the Horizon Europe funding in the first 3 years (2021-2023) and around one-third of all Horizon Europe participants were classified as SMEs. Not all SMEs are private, for-profit companies. Not all SMEs produce goods or services but they can be active in consultancy services, for instance SMEs specialised in managing R&I research projects. SMEs rarely coordinate projects and the ones that do coordinate are not predominantly active in manufacturing, but in project management and consultancy services.
- Most SMEs participate in Pillar II of the Programme 'Global challenges and European industrial competitiveness', followed closely by the SME-focused pillar III (predominantly from the European Innovation Council). The most distinctive role of private for-profit SMEs in Pillar II is that of technology developer and testing or validation of approaches and ideas. They are also frequently involved tasks related to the communication and dissemination of research results.
- Private for-profit SME participants are less likely to provide their own technology infrastructure, to take the lead in project management and to be involved Intellectual Property Rights management including technology transfer. The latter could be seen as counterintuitive, as one would expect SMEs to be more concerned or active in protecting Intellectual Property Rights from being disseminated unrestrictedly in the public domain.
- SMEs also significantly contribute to the Marie Skłodowska-Curie actions (MSCA), with 1251 participants. Despite this, most do not receive EU funding: nearly two thirds are unfunded. In about half of these cases, SMEs act as associated partners in MSCA Doctoral Networks, which train PhD candidates for careers outside academia, particularly in industry.

Source: The author.

[127] Sirtori et al. (2024), *SMEs and Open Strategic Autonomy.*
[128] European Commission (2024), Annual Report on European SMEs 2023/2024.
[129] European Commission (2024), 'Mission Letter for Commissioner Ekaterina Zaharieva from President Ursula von der Leyen*'.*
[130] European Commission (2024), SME participation in Horizon Europe – Key figures (and key issues) in the first three years.
[131] The label SME is used when the 'SME flag' has been applied under the R&I Framework Programme taxonomy that is based on a SME self-assessment. Start-ups in the context of Horizon Europe are included in the SME flag. Cf. https://webgate.ec.europa.eu/funding-tenders-opportunities/display/IT/SME.

Box 4: Role of SMEs in European Defence Fund (EDF)

Defence value chains in Europe have historically been characterised by limited cross-border cooperation[132]. The European defence ecosystem has traditionally been a closed system dominated by a small number of large defence contractors and several hundreds specialised defence-focused SMEs.

In recent years, EDF and national defence funding programmes for research or development projects aim to explore innovative defence concepts or adapt existing technologies for defence applications and improve cross-border collaborations. The European defence ecosystem is evolving into a more open and collaborative space. Newcomer SMEs, as well as research institutes, without a portfolio of defence technologies, but with multi-purpose innovative technologies are playing a greater role in exploring and developing novel or alternative defence use cases based on civil or dual-use technologies.

SMEs can participate in EDF funding programmes by either leading or joining consortia in SME-dedicated research or development calls, by partnering in broader thematic calls, or by taking advantage of cascade funding opportunities that lower entry barriers. Other EDF incentives aim to provide direct financial support or access to business coaching and testing facilities, helping innovative companies bridge the gap between concept and market-readiness. EDF is the overarching funding mechanism established by the EU to support collaborative defence research and development, while the EU Defence Innovation Scheme (EUDIS) is a specific component of the EDF that focuses on innovation and easing entry barriers for smaller companies.

Contrary to Horizon Europe, there is no R&I Dashboard available (yet) for retrieving statistics on the involvement of SMEs in EDF funding. Partial reporting on the EDF funding for collaborative research and development projects indicate that on average in 2021 and 2022 32% of the participants are SMEs and SMEs receive 19% of the EDF budget, which amounts to EUR 340,87 million[133].

Source: The author.

As there is currently no mechanism to identify dual-use potential of projects funded under Horizon Europe or EDF, there is no fixed methodology to assess the involvement of SMEs in dual-use R&I. A 2020 study report by the Joint Research Centre suggests a methodology to review granted projects with innovation fields with significant dual-use potential. This study indicated that over 50% of the participants contributing to dual-use projects are private for-profit listed entities. This study did not differentiate within this category between SMEs and larger companies and tech giants[134]. Another possibility would be to review granted project titles with SMEs involved and with query keywords identified by the TIM Dual-Use Index[135]. Compared to the 2020 study report, the TIM DU Index is (much) closer to the terminology used in the EU dual-use control list and terminology linked to emerging technologies that are not listed but with potential dual-use applications.

General challenges

SMEs, including start-ups and relevant scale-ups, are integral to the R&I landscape, driving technological advancements and economic growth. Their participation in EU R&I programmes can be challenging as outlined by several reports and articles[136,137]. Some key challenges relate to the following:

- Engaging within EU R&I funding programmes involves navigating competitive, time-sensitive and complex application procedures. SMEs, including start-ups and relevant scale-ups, often lack the specialised expertise required to develop detailed proposals that meet evaluation criteria. The administrative demands related to compliance and reporting can be substantial,

[132] European Commission, 'Defence SMEs', available at: https://defence-industry-space.ec.europa.eu/eu-defence-industry/defence-smes_en.
[133] Masson (2024), 'European Defence Fund: Beneficiary profile after two calls for proposals (2021-2022)'.
[134] Bordin et al. (2020), *Horizon 2020-funded security research projects with dual-use potential: An overview (2014-2018).*
[135] TIM Dual-Use Platform. Available at: https://knowledge4policy.ec.europa.eu/text-mining/tim-dual-use_en.
[136] European Commission (2021), Study on the effectiveness of public innovation support for SMEs in Europe – Final report.
[137] Bertello et al. (2022), 'Challenges to open innovation in traditional SMEs: an analysis of pre-competitive projects in university-industry-government collaboration'.

taking time and resources away from core business activities, in particular when manufacturing items.

- Navigating the complex regulatory environment of the EU presents another layer of difficulty for SMEs, including start-ups and relevant scale-ups. demands specialised legal expertise that many do not possess in-house. Start-ups, in particular, are vulnerable to overlook regulatory requirements dealing with novelties in their early days of existence. Collaborative projects introduce additional complexities in negotiating intellectual property rights and technology transfer agreements, especially when partnering with larger institutions. Moreover, adherence to state aid rules can limit the ability of SMEs, including start-ups and relevant scale-ups, to secure funding from multiple sources, restricting their financial flexibility and capacity to innovate.
- EU R&I projects often require SMEs, including start-ups and relevant scale-ups, to collaborate within consortia comprising universities, large companies, and other SMEs. Establishing these partnerships can be tough, as they may struggle to identify and connect with potential partners whose interests align with their own in the short time period drafting a proposal. Securing a leading role within such consortia is particularly challenging, with power imbalances often favouring larger organisations.
- Bridging the gap between research activities and actual product development remains a persistent issue, often due to insufficient resources and support structures. Additionally, opportunities to attract venture capital and private investment for scaling innovations are often limited, further constraining the growth potential of SMEs, including start-ups and relevant scale-ups, and their ability to compete in broader markets.
- SMEs, including start-ups and relevant scale-ups, and research organisations collaborating in EU-funded R&I programmes may have differing approaches to knowledge valorisation. Academic institutions often prioritise the dissemination of research results to advance scientific knowledge, while industry partners, including SMEs, may focus more on protecting intellectual property (IPR) to build up or maintain competitive advantage. Research and Technology Organisations (RTOs) and SMEs within the same consortium may have competing interests concerning exclusive and non-exclusive licensing of research results.
- Under funding programmes, beneficiaries have several obligations regarding their project results. These obligations revolve around dissemination, protection, and exploitation, ensuring that publicly funded research benefits society while safeguarding strategic and commercial interests.

Overall, these tensions underscore the need for clear communication and mutually agreed-upon strategies to balance the diverse objectives and constraints of SMEs, larger companies, and research organisations in EU-funded R&I collaborations.

As many SMEs, including start-ups and relevant scale-ups, are not recurring participants in R&I funded collaborations, they can benefit from support, such as the Horizon IP Scan[138], to develop agreements that protect their Intellectual Properties (IP) while also enabling them to share their knowledge and expertise. The 2024 Horizon IP Scan Study Report, however, highlights that SMEs face difficulties to make use of such advisory services due to restrictions imposed during the process of Consortium Agreement negotiations or beyond the completed contractual period. In addition, there is still a biased mindset amongst some SMEs that IP is considered to be less of a strategic task and rather a singular management action to solve a particular IP issue[139].

EUDIS spin-in calls focus on the faster uptake of innovative solutions from civil applications to defence use. It needs to build on results generated in a civil EU-funded R&D programme[140].

[138] Horizon IP Scan, available at: https://intellectual-property-helpdesk.ec.europa.eu/services/horizon-ip-scan_en.
[139] European Commission (2024), Horizon IP scan – Helping SMEs manage and valorise intellectual property in R&I collaborations.
[140] European Commission, 'EUDIS: Spin-in Calls'.

Moreover, the beneficiaries should have the rights to use these results, although this is dependent on the background and foreground information arrangement laid down in the Grant Agreement and Consortium Agreement of the initial funded project(s) and can be challenging in a diverse academia-industry knowledge valorisation setting.

Export control awareness challenges

Guidance to create awareness about export controls is available in various formats:

Box 5: Examples of awareness guidance on dual-use or military export controls

- Finland (2024) - Export control of dual-use items. Obligations for companies
- Japan (2025) - Security Export Guidance with special attention to SMEs
- United Kingdom (2021) - Guidance on exporting military or dual-use technology: definitions and scope
- Norway (2025) - Export control of knowledge transfer and international sanctions
- European Commission (2021) - The Defence Transfers Directive Handbook for SMEs
- European Commission (2025) - EU Sanctions Helpdesk for SMEs including red flags on dual-use items

Source: The author.

In recent years, the European Commission and the EU Member States have acknowledged the export control awareness and implementation challenges. To support industry and academia to get a better understanding of the impact of dual-use export controls on commercial and research activities, they have issued two guidance documents accordingly:

- Commission Recommendation (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009 focuses on industry, including SMEs, and how to proportionately develop and maintain internal compliance measures when dealing with dual-use items[141].
- Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items targets the academic sector with awareness guidance for researchers and internal compliance measures guidance for compliance officers within research organisations[142].

There is a noticeable difference between the 2019 and 2021 guidance documents: while the first one limits itself to support for industry to setting up and maintaining an Internal Compliance Programme, the latter goes a step further and additionally provides awareness guidance for researchers to understand the scope and impact of export controls on research (related) activities. The basic understanding info in the latter guidance can also be of relevance for industry facing export control challenges.

Despite these efforts, there remain some misunderstandings regarding the impact of export controls in the research context. The table below sums up some and indicates why they are inaccurate.

[141] Commission Recommendation (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009.
[142] Commission Recommendation (EU) 2021/1700.

Table 4: Clarifying misunderstandings on export control in research context

Misunderstanding	Clarifying the misunderstanding
The research project is funded by the EU or a national funding agency, therefore it is not subject to export controls.	Public funding sources do not exempt beneficiaries from export controls[143].
The end-user of the research result is the funder. It is up to the funder to apply for an export licence if the funder wants to make the results publicly available.	Export control responsibility lies with the entity that has the exporter role, not the funder role. If the beneficiary transfers controlled goods, software or technology to a foreign entity, the beneficiary acts as the exporter and is responsible for obtaining the export license[144].
The research results have to be published. Therefore, export controls do not apply.	Export controls have to take place before the research results are brought into the public domain. But only when the research results are specific enough to be captured by the control threshold[145].
The research results are not classified, hence they are not subject to export controls.	Export controls apply to both classified and unclassified controlled dual-use technology. Security-sensitive classified information and controlled dual-use technology may overlap in content. The security classification status and export control status may reinforce each other to safeguard research results against the unauthorised disclosure, including to third countries.[146]
The research is in an advanced technology area, it cannot be in scope of export controls.	Export control lists are dynamic and involve many legacy technologies with longstanding industrial supply chains, but they also include cutting edge technologies linked to quantum computing or to advanced semiconductor chip designs.[147]
The U.S. research partners do not need an export licence because of fundamental research[148], hence this applies as well for the EU research partners.	The U.S. fundamental research exemption does not automatically apply to EU research partners. While the EU export control system also foresees exemptions for basic scientific research and in the public domain, the EU scope is not as broad as the U.S. approach[149].

[143] According to Commission Recommendation (EU) 2021/1700, the source of research funding cannot be used as sole-indicator for determining whether the research involving dual-use items meets the technical control thresholds.
[144] The exporter is determined by the "exporter" definition in Regulation (EU) 2021/821.
[145] See Commission Recommendation (EU) 2021/1700 for more guidance on the applicability of the defined term "in the public domain" in Regulation (EU) 2021/821.
[146] According to Regulation (EU) 2021/821, some authorisations for lower-risk transactions, namely Union General Export Authorisations EU004 and EU008, cannot be used in case the dual-use item is classified equivalent to or above a certain security classification.
[147] See European Commission (2023), 'EU enables coordinated export controls by compiling national lists'.
[148] The fundamental research definition under EAR means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons. This includes research that is intended to be published but it does not include items other than technology or software. See Bureau of Industry and Security, 'Export Administration Regulations – Scope of the Export'.
[149] See European Export Control Association for Research Associations (2022), 'Comments to EU-US Trade and Technology Council' s Export Controls Working Group' for a summary of the key differences between the U.S. and EU approaches about this topic.

Misunderstanding	Clarifying the misunderstanding
A consortium with EU-only members cannot be subject to export controls.	Export controls do not only cover items leaving the EU. Annex IV of the EU dual-use regulation[150] deals with sensitive items that requires an authorisation for intra-Union transfers of dual-use items. If the research deals with such items, then export controls are relevant.

Source: The author.

These misunderstandings may have a spill-over to other consortium partners, like industry partners with limited knowledge about export controls in a funded R&I context.

Applicants and beneficiaries of funded R&I projects may (rightfully) claim that export controls are not applicable to them for various reasons[151].

- Firstly, research that is specially designed or modified for military use is not eligible for funding due to the exclusive focus on civil applications in Horizon Europe. Therefore, military export control scrutiny is indeed out of scope.
- Secondly, performing export controls for dual-use R&I in the project can indeed be not relevant because:
  - the research is not related to dual-use items that are subject to export controls.
  - the research materials and deliverables are not specific enough for the development, production or use of listed dual-use items[152].
  - the research and material deliverables are specific enough, but confidentiality or security classification restrictions refrain the deliverables to be exported or submitted into the public domain.
  - EU-only partners exchange other items than those in Annex IV of the EU Dual-Use Regulation[153] during the research, hence without exporting any item outside the EU.
  - There are no end-users or end-uses of concern as laid down in the so called 'catch-all provisions' of the EU dual-use list, including no trigger by any of the relevant competent export control authorities that a licence authorisation is required.
- Thirdly, the beneficiary may be aware of dual-use export controls but sees a low burden because it can make use of or possesses already one of the required licences. An EU general licence tailored specifically for EU-funded projects is sometimes proposed as a way forward to alleviate export control burden[154]. This is not foreseen in the current EU dual-use regulation. Such licence cannot relieve impacted beneficiaries from performing item classification to

[150] Regulation (EU) 2021/821.
[151] The list of reasons mentioned here should not be understood as exhaustive.
[152] The dual-use export control system has specific technical descriptions for tangible items and definitions concerning the development, production or use of intangible dual-use items. This is needed to determine if the research is specific enough to be considered as a controlled dual-use item. See Regulation (EU) 2021/821 for these technical descriptions and definitions, and Commission Recommendation (EU) 2021/1700 further explaining their impact in the context of research involving dual-use items.
[153] The Annex IV list of the EU Dual-Use Control List is a subset of particularly sensitive dual-use items that are subject to stricter export controls compared to other items listed in Annex I to Regulation (EU) 2021/821. While many items can be freely transferred within the EU without a license, Annex IV items require an export license even for intra-EU transfers (between EU Member States).
[154] See section 2.2. on Research performing organisations for this suggestion.

specify for which items the “research licence” and related reporting obligations would be needed.

- Fourthly, the beneficiaries can be in the misunderstanding that receiving an EU or national grant is exempting them from export control due diligence, including item classification, involved research partners screening and verifying whether research can be made available during or at completion of the research collaboration. Alternatively, the beneficiaries can be in the misunderstanding that export control obligations are only relevant for the coordinator and not for individual members.
- Lastly, neither the coordinator nor the impacted consortium member(s) may feel the need to go into export control details, as applying for a licence and complying with the licence conditions are time consuming and there is a (perceived) lack of enforcement against violating export control regulations in the research context. Obviously, this is not an appropriate reason for lacking export control awareness.

Below are two technology examples, one from EDF and one from Horizon Europe, to illustrate the need for awareness and vigilance of applicants and beneficiaries to take export controls seriously, when the technology scope is clearly dual-use.

Box 6: Two dual-use technology examples

Thermal imaging technologies

Thermal imaging technologies are used in a wide range of civil, security, and defence applications. Infrared detectors are a useful example to explore the classification challenges related to dual-use export controls or military export controls. The performance of infrared detectors is not only depending on the photodetector part, but also on the so-called Read-Out Integrated Circuit (or ROIC), which converts the electrical current from photodetectors into digital values for further (external) image processing.

Both photodetectors and ROICs are subject to dual-use export controls when meeting the technical specifications in the EU dual-use control list. In case they are specially designed or modified for military infrared imaging equipment then they are not listed on the EU dual-use control list but on the Common Military List of the EU.

Considering the call topic in EDF-2025-DA-SENS-IRD-STEP: Technologies for optronic detectors[155], there is no requirement stipulating that the photodetectors and ROICs need to be checked against dual-use or military export controls, neither is there a requirement that it should be focusing on the dual-use variant, the military variant or the variant free from export control requirements.

Without such an export control flagging in this call, beneficiaries can have a blind spot for export control requirements. EDF work programmes 2021 and 2023 also focussed on strengthening the supply chain for various infrared detector technologies.

Cryogenic chip technologies

Cryogenic chip technologies are promising solutions for quantum computing, space applications and cryogenic sensing.

Making use of the Horizon Dashboard[156], 9 projects have been identified to cryogenic semiconductors or detectors. Out of these 9 projects, 5 included SMEs and 4 did not.

In 2024, an increasing number of EU Member States and third countries have adopted national export controls on specified cryogenic integrated circuits, parametric signal amplifiers, cryogenic cooling systems and components and cryogenic wafer probing equipment. All the mentioned projects are still ongoing when this report was written and thus are confronted with the question whether these new export controls may impact some of their activities or the dissemination of the research results.

This example illustrates how projects can be without impact from export controls at the time of drafting, granting or start, but may be impacted during the execution of the project plan.

Source: The author.

[155] See European Commission (2025), Annex to the Commission Implementing Decision on the financing of the European Defence Fund and the adoption of the work programme for 2025 - Part 2 and amending Implementing Decisions C(2023) 2296 final and C(2024) 1702 final as regards financial support to third parties.
[156] European Commission, Horizon Dashboard – R&I Projects. Available at: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard.

Export control implementation challenges

SMEs, including startups and relevant scale-ups, just like larger companies and research organisations, face technical, administrative, legal and logistical challenges related to export controls. SMEs, including start-ups, due to their size and often more limited number of items in their portfolio, could tailor their compliance programmes better than larger companies. But they also tend to have less expertise and the contacts with government officials than that would be found in a multinational entity[157]. Scale-ups may experience and additionally export control burden when they are expanding internationally. Smaller companies may struggle to keep business and compliance tasks free from conflicts of interests as the same person takes up various responsibilities.

This section focuses on three key export control implementation challenges: item classification, TRLs as a means to perform export controls, and flows of items between EU partners and partners from associated countries. While they are not unique for SMEs, including startups and relevant scale-ups, they are as relevant for them as for other stakeholders when dealing with export controls.

Item classification

Without successful item classification, it is very difficult to assess if an export license is required. For dual-use items, other than those in Annex IV[158], this means that in most cases the transfer of dual-use items inside the EU or the mere use of a dual-use item inside the EU does not require export controls as there is no 'export', including transmission of technology, outside the Customs Territory of the European Union.

The complexity in research projects, however, is that a consortium partner outside the EU may receive (get access to) controlled goods, software or technology, or the dissemination of project results / deliverables may be released into the public or commercialised after the project with customers outside the EU. These activities then may trigger export controls.

A key feature of dual-use export controls is that it requires matching technical specifications of research items with the dual-use control list, as items on this list have a known civil application and a known or suspected use in the context of Weapons of Mass Destruction, conventional military systems, terrorism, cybersurveillance or human rights violations. The dual-use control list foresees some hardware specific decontrols, but also exemptions for software and technology that is already in the public domain and for technology that is the result of basic scientific research.

For military export controls, the classification aspect is not so straightforward. The EU export control system for defence-related items ('military export controls') is governed primarily through national implementation of Directive 2009/43/EC and Common Position 2008/944/CFSP[159].

A military item is covered by the Common Military List of the EU or an additional control list from an EU Member State. Key requirement is that the item (goods, software or technology) must be 'specially designed for military use' or 'modified for military use'. Both terms are undefined and there is no uniform guidance how to interpret this, given the national competence of EU Member States in this area. Possible indicators include (but by no means are harmonised across the EU):

---

[157] Bauer et al. (2017), *Challenges and good practices in the implementation of the EU's arms and dual-use export controls: A cross-sector analysis*.

[158] The Annex IV list of the EU Dual-Use Control List is a subset of particularly sensitive dual-use items that are subject to stricter export controls compared to other items listed in Annex I to Regulation (EU) 2021/821. While many Annex I items can be freely transferred within the EU without a license, Annex IV items require an export license even for intra-EU transfers (between EU Member States).

[159] Unlike Regulation (EU) 2021/821, this Common Position is not directly binding but sets common criteria that EU Member States must consider when issuing export licenses for military goods. The EU Common Military List sets a reference for national control lists. While dual-use export controls are civil trade controls governed under the common commercial policy of the European Union, military controls are foreign policy and security competences at EU Member State level. Both types of items are governed by different regulatory frameworks, including licence applications, reporting modalities and guidance.

- first-intent design (design, prototyping or manufacturing with a military end-use application in mind),
- developed or modified upon request of a defence actor or a defence funding actor[160],
- design characteristics or modifications beyond commercial (off-the-shelf) characteristics (such as dimensions, materials, operational requirements related to dust, shock, temperature, radiation, electromagnetic pulse, etcetera),
- rated according to a military standard, or
- as decided by the competent authority of the EU Member State.

The difficulty here is that there is no EU guidance, contrary to the U.S. guidance, about the meaning of "specially designed", not in the context of the dual-use export control and not in the context of military export controls[161].

The last indicator '*as decided by the competent authority of the EU Member State*' is particularly challenging because of diverging interpretations and practices on the design or modification criteria for military items by the competent authorities. The lack of (harmonised) guidance further complicates the predictability for beneficiaries to assess whether they are subject to export controls or not.

Diverging national control provisions and practices in EU Member States, including classification and end-user assurances, hinder the smooth flow of controlled items in EU-funded research projects involving multiple export control authorities.

This section concludes with an example to illustrate how item classification is a challenge.

Box 7: Example of item classification challenges

Unexploded ordnance (UXO) refers to explosive weapons such as bombs, landmines, grenades, or artillery shells that failed to detonate after they were deployed. UXO can remain dangerous for years or even decades, posing serious risks to civilians, military personnel, and infrastructure. Specialised bomb disposal teams from the military, but also from Non-Governmental Organisations (NGOs) and government organisations work to locate, remove, and safely dispose of UXO. A key challenge is to detect UXO. There are various technologies available.

This example focuses on multispectral and hyperspectral imaging attached to drones to detect subtle ground changes caused by buried explosives. These imaging have advantages compared to other imaging technologies, radar technologies or magnetic detectors and analyse hidden material signatures of buried UXO, disturbing soil layers when buried, affecting moisture retention and plant growth. As such, this application is related to the detection of explosives but not related to the actual (military) activity of sweeping explosives.

UXO items are military items, listed under category ML4.a of the Common Military List of the European Union[162]. Equipment specially designed for military use and specially designed for the detection of mines are listed under ML4.b. ML4.b also controls specially designed components of such equipment. Infrared or thermal imaging equipment specially designed for military use and specially designed components therefore, but not specially designed for detecting mines are controlled under ML15. Depending on the funding programme requirements, such military equipment and components cannot be in research scope or must be in research scope.

Non-military hyperspectral cameras, detectors and drones can also be used to detect UXO and need to be checked against the EU dual-use control list[163].

If the research is focused on sensor fusion or imaging software solutions helping in detecting, classifying and mapping UXO, or on AI solutions for automating and improving accuracy searches, then the item classification is not straightforward or even not applicable.

[160] It is interesting to note here that the United States Munitions List contains items that are subject to the International Traffic in Arms Regulations (ITAR) solely because they have been funded by the Department of Defence. Such classification trigger is not present in the Common Military List of the European Union.
[161] For the U.S. definitions on specially designed, see https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.41 in the context of ITAR and https://www.bis.gov/ear/title-15/subtitle-b/chapter-vii/subchapter-c/part-772/ss-7721-definitions-terms-used-export in the context of EAR.
[162] Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment, L 335.
[163] See technical descriptions 6A002, 6003 and 9A012 in Annex I to Regulation (EU) 2021/821.

Even if there are items identified that are considered listed dual-use or military items, then the consortium needs to review the research activities and assess whether it deals with the development, production or use of these items, and whether the flow of items in during the research triggers export control obligations.

This example illustrates the multiple checks and steps to take to confirm or exclude that the research may deal with or result in export-controlled items.

Source: The author.

Research involving dual-use items - TRLs

EU guidance on research involving dual-use items[164] refers to Technology Readiness Levels (TRLs), a non-discipline specific measurement system with a scale from 1 to 9 with indicators from of the maturity level of particular technologies, to assist practitioners in determining whether the research output in the form of technology (not in the form of tangible goods or software!) can be considered as basic scientific research or not. If so, then the export control regulation exempts this research output from authorisation requirement. This EU guidance states that:

- research output stemming from TRLs 1 and 2 research is generally considered basic scientific research.
- research output stemming from TRLs 3 and 4 needs to be assessed on a case-by-case basis.
- research output stemming from research above TRL 4 is not considered as basic scientific research.

There is however also national guidance available, such as the German Manual Export Control and Academia[165]. This guidance also uses TRL levels but does not draw identical conclusions as the EU guidance: the German guidance states that TRL levels 1 to 3 are typically basic scientific research, while TRL levels above 3 are considered applied research. Obviously, such (subtle) differing in guidance further complicates a level-playing field inside a consortium with partners from different EU Member States.

Innovative ideas and university level concepts are generally considered TRL 2 or 3, technology validation in a laboratory environment, (pre-commercial) industrial prototypes and demonstrators are considered TRLs 4, 5 or 6, and beyond that it goes until TRL level 9 where it reaches the stage of a commercial technology. For instance, the European Innovation Council (EIC) Pathfinder aims projects with TRL 1 or 2 to reach TRL 3 or 4. The EIC Transition fund focuses on supporting the demonstration of technology in application-relevant environment and to develop business and market readiness in the TRL 3-6 range. The EIC Accelerator fund, on the other hand, is targeting innovation activities in the TRL 6-8 range[166].

As SMEs, including startups and relevant scale-ups, are often involved as contributing to the prototyping, testing or demonstrating innovative products, they are likely to not meet the basic scientific research exemptions and thus require particular attention to export controls for dual-use items. For them as well, the guidance on the use of TRLs to support export control due diligence has to be as harmonised as possible across the EU.

Flows between EU partners and partners from associated countries

As mentioned above, export controls require a controlled activity in addition to a controlled item. The research activities of a consortium with only EU-based partners are much less subject to export controls during execution, then a consortium with both EU based and non-EU based partners.

Looking at Horizon Europe data in the 2021-2025 period, 88,3% of SMEs come from EU Member States, 8,3% comes from Associated Countries (top 3: United Kingdom, Norway and Israel count

[164] Commission Recommendation (EU) 2021/1700.
[165] BAFA (2023), 'Manual - Export Control and Academia'.
[166] EIC Funding opportunities, available at: https://eic.ec.europa.eu/eic-funding-opportunities_en.

for 73%), and 3,5% comes from Third Countries (top 3: Switzerland, United States and South Africa count for 80%)[167].

Below are some examples how the involvement of associated or third country partners may trigger more export control vigilance:

- EU-based SME sends a design file of a controlled electronic item to a foundry outside in a third country.
- EU-based SME sends a sample for inspection or metrology purposes to a partner in an associated country.
- EU-based SME makes available controlled technology from a cloud-storage located inside the EU to a non-EU based partner.

Associated or third countries have their own export control systems, not necessarily aligned with the EU export control system. Hence, constellation of partners can trigger export control requirements from both the EU and the non-EU side.

Some jurisdictions, notably the United States of America, are known for their extraterritorial effect and higher degree of complexity compared to the EU export control systems. The Export Administration Regulations (EAR) regulates the export of dual-use items, while the International Traffic in Arms Regulations (ITAR) focuses on military items. Even without being subject to EU or EU Member States export controls, export controls can become relevant if the research makes use of U.S. origin items or EU-made items that are the direct product of controlled U.S.-origin technology or software, or produced in part with equipment that is the direct product of specific types of US-origin technology or software, to the EAR jurisdiction. This requires highly specialised knowledge to navigate which is often not present in many SMEs, including startups and relevant scale-ups.

Timing aspect when to discuss export control related aspects

Horizon Europe funding calls appropriately require applicants to confirm that, if their project involves dual-use items as defined under Regulation 2021/821, they will adhere to the relevant regulatory framework.

It is important to note that export controls are not violated merely by the submission, approval, or execution of a research proposal involving dual-use items. The regulatory framework governing export controls is only triggered when controlled items are subjected to specific activities- such as export, transfer, or technical assistance - without the appropriate authorisation or exemption.

A preliminary export control scan during the drafting phase of the project proposal is advisable for a few higher risk indicators, such as:

- the project will involve partners from non-EU countries.
- the project will involve nuclear related items.
- the project makes use of U.S. items, including equipment, software or designs.
- the call puts restrictions on the dissemination of results due to security considerations
- the call targets technologies with recurring export-controlled items, such as specialised semiconductor manufacturing technologies, quantum computing, sensing or communication, cybersecurity, advanced materials, nanotechnology, biotechnology, synthetic biology, advanced computing chips for artificial intelligence or data centres, aerospace, drones and propulsion engines.

[167] Own analysis from Horizon Europe Dashboard for projects with start date in period 2021-2025. Data retrieved via: https://dashboard.tech.ec.europa.eu/qs_digit_dashboard_mt/public/sense/app/d58f3864-d519-4f9f-855e-c34f9860acdd/sheet/QCdc/state/analysis.

This early-stage assessment can help identify that the project may be subject to export controls. The project coordinator can take the initiative at the outset to inform consortium members about the fundamental principles of export controls. This early awareness can help in pinpointing high-risk activities or deliverables that may require specific regulatory attention.

Consortium members affected by export controls should carefully consider the optimal timing for obtaining the necessary authorisation(s). Given that obtaining export licenses can be a time-consuming process, the early preparation is key to avoiding disruptions to project timelines. By integrating export control considerations into project planning from the beginning, beneficiaries can ensure smoother project execution while remaining fully compliant with the regulatory framework.

2.3.4. Opportunities to increase awareness on export controls in R&I

Building on existing security requirements in EU funded programmes for beneficiaries

Before turning to the opportunities for increased participation and awareness on export controls in R&I, this section sums up the existing security safeguards and highlights where export control considerations are already embedded.

The current security safeguards in Horizon Europe Regulation[168] include:

- Article 20: security screening procedure for projects involving sensitive or classified information, or information or materials subject to national security restrictions.
- Article 22.5: call limitations or exclusions for entities based in certain third countries, or owned or controlled from certain third countries.
- Article 39: exploitation and dissemination following the 'as open as possible, as closed as necessary' principle.
- Article 40: the right of the European Commission or funding body to object to transfer and licencing of results to non-associated third countries or when not in line the EU's interests.

The following guidance notes have been introduced for applicants to submit proposals for Horizon Europe, Digital Europe and EDF programmes:

- The **'***Guidance note - Research with an exclusive focus on civil applications'*[169] states that in case the proposed research activities involve dual-use items, in the sense of Regulation 821/2021, the applicant will comply with the related legal obligations (e.g. export/import licences etc.) prior to the use, import/export of these items. While such statement can support dual-use export control awareness, it does not lead to any more systematic follow-up. Since this check is outside the security review or ethics self-assessment, it is also not an aspect that is included in the proposal evaluation by the independent experts[170].
- The *'Guidance note - Potential misuse of research'*[171] highlights that misuse of research results is a cross-cutting issue and therefore there is attention in both the ethics-self assessment and the security review. It is not easy for beneficiaries to come up with the potential for misuse of research, because it is not linked to the benign intention of research plans but to the usefulness of its research results for actors with nefarious intentions.

[168] Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013.
[169] European Commission (2021). 'Guidance note - Research with exclusive focus on civil applications*'.*
[170] See European Commission (2021), 'The Ethics Appraisal Scheme in Horizon Europe', slide 21, stating that 'For dual use, the declaration by the applicant is sufficient (no further checks in evaluation or grant management)".
[171] European Commission (2021), 'Guidance note - Potential misuse of research'.

- The *ethics self-assessment* requires applicants to make a risk assessment and risk mitigation at the stage of application, with recommendation to appoint an ethics advisor or advisory board. One example of misuse of research results is the development of surveillance technologies that could curtail human rights, an explicit focus as well of the revised dual-use Regulation 821/2021. Specifically, the ethics self-assessment contains a section on Artificial Intelligence (AI) for applicants to review if the use of AI is intended for a(n) (autonomous) weapon system for EDF applications.
- The *'Guidance note - How to handle security-sensitive projects'*[172] requires applications to review the risks concerning the potential for misuse of results (including in relation to crime, terrorism, or in the development of chemical, biological, radiological or nuclear (CBRN) weapons and the means for their delivery), and the involvement of information and/or materials subject to national security restrictions. There is no cross-reference to items subject to dual-use or military export controls, even though items with the capabilities to contribute to such security applications are included in the control lists. Similarly, a mentioned misuse category is the development of materials/methods/technologies and knowledge that could harm humans, animals or the environment if they were released, modified or enhanced. Again, the dual-use regulation contains a significant amount of chemicals, bacteria, viruses and toxins that can do harm to plants, animals and humans.

The EDF 2025 call[173] contains several interesting observations how export controls are relevant to applicants to consider when drafting a proposal:

- The explicit requirement to provide a product free from export control restrictions by non-EU or non-EDF Associated countries in order to bolster EU sovereignty and independence (EDF-2025-RA-ENERENV-PSR: Propulsion system for next generation rotorcrafts).
- The option for the development of generic Digital Twin models which are not to be subject to security or export controls (EDF-2025-RA-SIMTRAIN-DAFAS: Multi-Disciplinary design and Analysis Framework for Aerial Systems).
- The explicit requirement to providing recipients of financial support to third parties, in particular SMEs not previously active in the defence sector and able to adapt innovative technologies for soldier systems, with the necessary knowledge on (amongst others) export controls for doing business in the defence sector (EDF-2025-DA-PROTMOB-SS: Full-size demonstrators for next generation soldier systems and EDF-2025-DA-SI-GROUND-DAMM: Drone-based affordable mass munitions).

Additional opportunities to increase awareness

The Horizon Europe funding programme is currently in its second and final phase. The Commission published the Strategic Plan 2025-2027 and outlined 'a more resilient, competitive, inclusive, and democratic Europe' as a key strategic orientation. It also included a section on research security, but interestingly no reference to export controls[174]. Given the rapidly evolving geopolitical circumstances, the limited focus on export controls in international research collaborations is notable.

Funders can use export control lists to identify strategic dual-use technologies that require support, guiding investment towards areas with known use or high potential for civilian and military applications. In the other direction, export control authorities can tailor better from the wealth of innovative R&I to assess whether subareas of innovation areas are relevant for fine-tuning existing export controls or develop new ones. Some funding agencies, like Research Foundation Flanders

[172] European Commission (2021), 'EU Grants - How to handle security-sensitive projects'.
[173] See Annex to the Commission Implementing Decision on the financing of the European Defence Fund and the adoption of the work programme for 2025 - Part 2 and amending Implementing Decisions C(2023) 2296 final and C(2024) 1702 final as regards financial support to third parties.
[174] European Commission (2024), Horizon Europe strategic plan 2025-2027.

(Flanders, Belgium) have developed an approach to create awareness about research security when submitting a proposal. This research security includes a cross-reference to export controls[175].

Box 8: Research Foundation Flanders creating awareness on export controls through research security

Research Foundation Flanders adopted a Research Security Appraisal Tool and used the Call 2024 for joint research projects with China as test case. This tool will be expanded to other calls in 2025.

Researchers must complete a self-assessment questionnaire on research security aspects of the planned research, and if this questionnaire results in a high-risk evaluation, then a research security approval is needed from the host institution[176].

During the self-assessment[177], the researchers are asked to evaluate their research to the following 6 elements: 1. Attractiveness to the Knowledge Economy 2. EU Critical Technology 3. Military Aspects 4. Dual Use 5. Misuse 6. Interference.

While the outcome of the self-assessment is not influencing the outcome of the proposal assessment, it aims to trigger awareness amongst the proposal partners and their institutions. While research security considerations are not identical to export control considerations, there is some overlap, and such an approach can be beneficial to increase awareness about export controls for applicants and future beneficiaries.

Source: The author.

The adoption of (advanced) analytic tools by authorities can help with tracking patterns in research outputs linked to dual-use technologies. These technologies complement human oversight by providing data-driven insights that flag potential dual-use opportunities and concerns.

Funding agencies could facilitate beneficiaries to liaise with export control authorities to provide clarifications.

Programme officers or managers, such as the European Innovation Council Programme Managers, are involved in the active management of portfolios of funded projects targeting SMEs and dual-use technologies. Making training and awareness on key export control aspects for these Programme Officers or Managers available may support beneficiaries and may ease the liaising with the competent export control authority when relevant.

Inspired by the Horizon IP Scan[178], a Horizon Europe or EDF Export Control Scan service may could be foreseen offer export control first-aid support to questions arising at different stages of a funded project and facilitate more in-depth support by the competent export control authorities.

The TIM Dual-Use Index is a good basis for a dual-use flagging mechanism:

- for funders to highlight the dual-use potential, civil-military synergies or relevance for export control screening and facilitate monitoring or reporting on such calls.
- for applicants and beneficiaries of funding calls to consider export controls when drafting, negotiating consortium agreement or starting/executing/closing a project.
- for export control authorities to target their outreach, monitoring and enforcement efforts concerning R&I involving dual-use items.

It is important to create a practical set of index terminology, ideally emphasising key dual-use technologies. An overly large set of terms may significantly affect calls and projects with export control obligations. Once identified, these projects can be monitored more closely during their implementation. The standard Data Management Plan requirements can then help projects in monitoring their export control obligations.

Activities involving dual-use items or military items may trigger export controls and the control policies and procedures are not identical. The more funding opportunities will open up for dual-use

[175] Research Foundation Flanders, 'Research security'.
[176] Research Foundation Flanders (2017), 'General Regulations: Article 4ter - Research security'.
[177] Cf. Research Foundation Flanders (2025), 'Research Security Appraisal' for an illustration of the self-assessment.
[178] Horizon IP Scan, available at: https://intellectual-property-helpdesk.ec.europa.eu/services/horizon-ip-scan_en.

technologies with civil and defence use cases, the more beneficiaries will have to consider whether they are in scope of dual-use or military export controls. The current EU dual-use export control framework, in particular related to Intangible Technology Transfer controls, needs improvements to have an EU-level playing field in the research context. The European Export Control Association for Research Organisations (EECARO) is particularly active in this field[179].

As funding schemes promote cross-border cooperation between industry and academia in defence value chains, the harmonised interpretations concerning 'specially designed' or 'modified for military use', and harmonised rules for flows of defence-related items become essential.

The present guidance and support to beneficiaries, including SMEs, startups and relevant scale-ups, which may be impacted by export controls is scattered and limited. Some improvements are listed below:

- SMEs significantly contribute to the Marie Skłodowska-Curie actions (MSCA), focused on training and movement of high-potential (third country) researchers, by granting access to dual-use infrastructure and technologies. Awareness raising about the export controls in sensitive technology areas for the involved entities and researchers is useful.
- Defence related funding programmes or calls focusing on military use cases can clarify that the research they fund is to be checked against dual-use or military export controls.
- Dedicated calls involving dual-use technologies can request the applicants to include in their proposal how export controls will be managed for the execution of the project plan and how this will impact the management of project deliverables.
- Bundle best practices from granted projects where export controls played a relevant role in the execution can serve as an inspiration for future applicants.
- Provide basic training material on export controls that can be used in the context of granted project onboarding.
- Provide a guidance note how to deal with dual-use or military export controls alike other guidance notes reviewed above.
- Foresee that if the proposal is selected for funding, the export control review may result in specific contractual requirements in the Grant Agreement.

[179] See for instance the following position papers: EECARO priorities for the improvement of Intangible Technology Transfer controls, EECARO Feedback on the White Paper on Export Controls and EECARO Feedback on the EU White Paper R&D with dual-use potential. Available at: https://eecaro.eu/position-papers/.

3. Policy strategies supporting dual-use research and innovation – international examples and benchmarks

3.1. Introduction

Over the past decade, dual-use R&I has moved to the forefront of strategic policy discussions. Effective dual-use strategies aim to balance technological innovation with security and ethical considerations, so that progress in areas like artificial intelligence or biotechnology can drive economic and societal benefits while minimizing risks of misuse or proliferation. Countries that successfully integrate their civilian and defence innovation systems, while protecting the integrity of their research, are reaping benefits in agility and security. Global benchmarks underscore the importance of three pillars: a clear vision for technology foresight, seamless innovation pipelines linking civil and military sectors, and prudent openness or research security measures to protect sensitive knowledge.

Chapter 3 examines how leading nations and organisations have fostered dual-use R&I policy strategies over the past decade, with a focus on the past five years. It analyses international examples to identify trends and best practices that could inform policymakers and draw out strategic insights relevant to the EU context. The chapter is structured as follows: the first section introduces the context and analytical approach, the second section analyses global policy trends and strategic developments, whereas the third section presents international case studies across key regions. Finally, the fourth section offers a synthesis of strategic observations relevant to EU policy development.

The chapter is based on a targeted literature review covering government strategies, reports of think tanks and expert analysis, as well as strategic documents from key countries and institutions. The review covers the following actors in dual-use policy as international benchmarks: the United States, China, Japan, Republic of Korea, Israel and the United Kingdom, and EU Member States such as Germany, France, Finland, Italy, Poland, and Sweden. Insights from NATO and multilateral initiatives are also incorporated where relevant, given their influence on EU Member States' policies.

To structure the analysis, an analytical framework with three dimensions was used:

- *Technology foresight & prioritisation* – how nations set long-term R&I priorities and anticipate emerging dual-use technologies;
- *Civil–defence technology transfer* – how they facilitate the flow of innovations between the civilian and defence sectors; and
- *Research security and responsible internationalisation* – how they manage to mitigate security risks (e.g. export controls, intellectual property protection, foreign influence) while maintaining beneficial international research collaboration.

These dimensions reflect the key strategic and operational tensions that governments must navigate in dual-use governance — from prioritising technologies, to enabling effective innovation flows, to managing risk in a globalised research landscape. The framework guided the collection and comparison of country-specific information under each theme. Each country case was examined across all three dimensions to capture its overall dual-use strategy as summarised in table 4 below. Cross-cutting factors such as regulatory frameworks, intellectual property rights (IPR) management, and monitoring/enforcement mechanisms were noted as underpinning elements of these strategies.

Table 5: Summary of dual-use strategy in R&I across three policy dimensions

Country	Technology foresight and prioritisation	Civil-defence technology transfer	Research security and responsible internationalisation
United States	Well-developed and integrated dual-use foresight, strong industry-military alignment.	Strong civil-defence integration, venture capital and procurement-driven.	Security-driven with strict controls, focus on protecting critical tech.
China	State-driven, military-led foresight, tightly linked to defence priorities.	Fully integrated under Military-Civil Fusion policies.	Highly restrictive, centralised control over sensitive R&D.
Japan	Structured foresight, growing emphasis on national security applications.	Cautious but increasing civil-defence integration.	Risk-aware and shifting towards a security-first approach.
South Korea	Expanding foresight capacity, traditionally defence-heavy but evolving.	Early-stage civil-defence cooperation, focused on AI and semiconductors.	Balanced but tightening security controls in strategic sectors.
Israel	Security-driven foresight, clear alignment between commercial and defence tech.	Strong and well-institutionalised civil-defence technology flow.	Highly protective, selective international openness.
Germany	Strengthening dual-use foresight, with growing emphasis on defence R&D.	Historically civilian-led innovation but increasing alignment with defence needs through new agencies and EU projects.	Introducing research security frameworks, including export controls and IP protection.
France	Strategic foresight in defence but limited direct dual-use coordination.	Emerging integration, largely through defence R&D funding and European partnerships.	Security-focused but allows cooperation with select partners.
Finland	Focus on resilience in tech foresight, growing dual-use consideration.	Early-stage civil-defence cooperation, mainly in cybersecurity and emerging tech.	Open research climate with rising concerns over security risks.
Italy	Limited historical foresight in dual use but increasing focus due to geopolitical shifts.	Fragmented integration, leveraging EU defence initiatives to strengthen technology transition.	Strengthening controls on emerging tech exports, aligning with European security frameworks.
Poland	Developing foresight, defence-dominated but shifting towards dual-use thinking.	Growing civil-defence integration through funding and industry incentives.	Increasing security restrictions, selective openness.
Sweden	Strong civilian foresight but weaker alignment with defence needs.	Fragmented civil-defence integration, with growing but uneven initiatives.	Open research environment but introducing security filters.

Country	Technology foresight and prioritisation	Civil-defence technology transfer	Research security and responsible internationalisation
United Kingdom	Advanced foresight with explicit dual-use priorities.	Increasing civil-defence integration through public-private collaboration and dedicated funds.	Balanced, risk-managed openness with increasing security measures.

Source: The author.

In recent years, the integration of civilian and defence research and innovation (R&I) has become increasingly vital for national security and economic resilience. Countries around the world are adapting to this paradigm shift by aligning economic policies, fostering innovation ecosystems, and reinforcing research security. The comparative analysis of national strategies reveals a set of cross-cutting developments that offer insight into how governments are responding to shared challenges. These include the growing influence of civilian-driven innovation on defence capabilities, the complex task of anticipatory foresight amid geopolitical rivalry, and the need to balance openness with strategic control. Workforce development, ethical frameworks, regulatory oversight, and risk governance also emerge as key enablers of dual-use innovation.

The following observations distil these trends as seen across a diverse range of national contexts:

Blurring lines between civilian and defence innovation: Technological advancements in areas such as artificial intelligence (AI), biotechnology, and cybersecurity are predominantly driven by the commercial sector. Countries like the United States have embraced private sector solutions, exemplified by initiatives such as the Defense Innovation Unit (DIU)[180]. China's Military–Civil Fusion (MCF) policy tightly integrates civilian technological advancements into national defence[181]. These developments illustrate the growing convergence of civil and military technology origins[182]. However, some nations still struggle to adapt procurement and funding models to this new reality, risking innovation lag[183].

Foresight amid geopolitical rivalry: Geopolitical competition has intensified the focus on long-term planning in critical technologies. The United States and China have propelled extensive public investments in AI and semiconductors, reflecting a strategic race for technological supremacy[184]. Within the EU, foresight capabilities are evolving through efforts such as the Observatory of Critical Technologies and iterative planning under the Economic Security Strategy[185]. These developments reflect an increasing need for flexible, forward-looking mechanisms, potentially including AI-supported tools, to anticipate emerging technology trajectories[186].

Integrating economic and security policies: Nations are increasingly aligning economic instruments with security objectives to safeguard dual-use innovation. Strategic industrial policies, such as the U.S. CHIPS and Science Act and the EU's approach under the Strategic Technologies for Europe Platform (STEP), are designed to direct funding toward priority technologies while screening foreign involvement in sensitive areas[187]. While the STEP platform focuses on industrial

[180] González (2024), 'How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex'.
[181] Farrow (2023), 'Modernization and the Military-Civil Fusion Strategy'; and Joshi (2022), 'China's Military-Civil Fusion Strategy, the US Response, and Implications for India'.
[182] Baldwin (2024), *Critical Dual-Use Technologies: Commercial, Regulatory, Societal and National Security Challenges*.
[183] Gallo (2025), 'The Defense Innovation Ecosystem'.
[184] Draghi (2024), *The future of European competitiveness: A competitiveness strategy for Europe*.
[185] Matthews (2023), 'Europe Needs to Hone Its "Technological Edge" in Areas Where It Leads, Think Tank Fellows Say'.
[186] Draghi (2024), *The future of European competitiveness: A competitiveness strategy for Europe*.
[187] Van Hollen's office in the US Senate (2022), 'CHIPS and Science Act of 2022 Division A Summary - CHIPS and ORAN Investment'; Aharonov, and Lax (2024), 'חוקי השבבים של ארצות הברית ושל האיחוד האירופי (U.S. and EU Chip Laws)'; and Matthews (2023), 'Europe Needs to Hone Its "Technological Edge" in Areas Where It Leads, Think Tank Fellows Say'.

investment, other frameworks aim to embed economic security through updated trade, procurement, and investment rules[188].

Responsible internationalisation and trusted networks: In response to growing geopolitical concerns, countries are forming trusted partnerships that restrict access to critical knowledge and infrastructure. Initiatives such as AUKUS, NATO DIANA, and bilateral tech cooperation among like-minded states illustrate how international collaboration is being restructured along security lines[189]. These frameworks are supported by domestic safeguards, including investment screening and due diligence rules, as seen in countries like the UK, Finland, and the U.S.[190] The EU's Economic Security Strategy further reflects this perspective toward conditional openness[191].

Workforce and talent development: Effective dual-use R&I strategies emphasise cultivating talent that spans academia, industry, and defence. The United States promotes this through the SMART scholarships programme[192], while Germany's KIWi initiative supports science diplomacy and mobility[193]. Israel leverages elite military units such as Unit 8200 to generate technical expertise with civilian spillovers[194]. The EU's challenge remains retaining and attracting skilled personnel, particularly in AI and cybersecurity[195], and some European countries including the UK have begun experimenting with dedicated fellowships and startup visa schemes[196].

Ethical and normative considerations: The dual-use nature of emerging technologies raises significant ethical questions. Countries such as the U.S. and Germany have introduced ethical review boards and national guidance frameworks[197]. The EU's AI Act includes requirements for transparency, accountability, and rights-based safeguards. These efforts reflect a broader concern with ensuring dual-use innovation aligns with democratic norms, international law, and societal values[198]. Complementary frameworks such as Responsible Research and Innovation (RRI) continue to inform EU-level debates on ethical governance[199].

Monitoring and enforcement: Effective oversight mechanisms – including audits, export control systems, and regulatory inspections – are essential for ensuring compliance with dual-use rules. Countries such as the United States and Germany maintain stringent control systems to enforce IPR protection, safeguard sensitive technologies, and deter illicit transfers[200]. At the EU level, updated export control regimes and forthcoming initiatives under the EU's Economic Security Strategy reflect a convergence of civil and defence compliance tools[201].

---

[188] The U.S. Senate Committee on Foreign Relations (2024), *One Step Forward, Two Steps Back: A Review of U.S.-Europe Cooperation on China*; and European Commission (2023), *Joint Communication on European Economic Security Strategy*.

[189] Munro (2024), 'Tech Industry Is the New Defence Industrial Base'; and Baldwin (2024), *Critical Dual-Use Technologies: Commercial, Regulatory, Societal and National Security Challenges*.

[190] The League of European Research Universities (2023), 'Managing and Governing Risks in International University Collaboration'; and The U.S. Senate Committee on Foreign Relations (2024), *One Step Forward, Two Steps Back: A Review of U.S.-Europe Cooperation on China*.

[191] European Commission (2023), *Joint Communication on European Economic Security Strategy*.

[192] SMART, 'Scholarship-for-Service Program', available at: https://www.smartscholarship.org/smart.

[193] DAAD KIWi, 'KIWi at a Glance', available at: https://static.daad.de/media/daad_de/pdfs_nicht_barrierefrei/infos-services-fuer-hochschulen/kompetenzzentrum/dokumente/kiwi_at_a_glance.pdf.

[194] Kruppa, and Perry (2024), 'Silicon Valley's Hot Talent Pipeline Is an Israeli Army Unit'.

[195] Turp-Balazs (2025), 'The Brain Drain Challenge: Strategies to Retain Talent in Emerging Europe'.

[196] British Council, and Universities UK International (2024), 'Managing Risk and Developing Responsible Transnational Education (TNE) Partnerships'.

[197] JASON advisory group (2024), *Safeguarding the Research Enterprise*.

[198] Shih (2023), 'Responsible Internationalization - Why, What, and How?'.

[199] Schuch et al. (2024), 'Final Report of the Mutual Learning Exercise on Tackling Foreign Interference in Research and Innovation (R&I)'.

[200] Federal Ministry of Education and Research (2024), 'Position Paper of the German Federal Ministry of Education and Research on Research Security in Light of the Zeitenwende'; and Research Compliance Office, 'Research Security - FAQ for International Affiliations Foreign Engagements'.

[201] Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items; and European Commission (2023), *Joint Communication on European Economic Security Strategy*.

3.2. Strategic development in dual-use R&I

The development of dual-use R&I has evolved significantly in response to shifting geopolitical, economic, and technological landscapes. This section examines the evolution of dual-use R&I strategies, tracing key milestones that have shaped national and international policies. It then explores global trends and approaches, identifying commonalities and divergences in how nations balance security imperatives with innovation-driven growth. Finally, the section delves into country-specific developments, highlighting the strategic choices made by different states to integrate dual-use technologies into their broader R&I ecosystems.

3.2.1. Evolution of dual-use R&I strategies

Since 2010, dual-use R&I strategies have evolved from fragmented efforts to more of an integrated, whole-of-government priority. Initially, national security and civilian innovation operated in largely separate spheres, but by the mid-2010s, shifts in geopolitics and technology forced governments to start rethinking their approaches[202]. By the 2020s, dual-use innovation has become a core pillar of national security policies, with technology viewed as both an economic asset and a security imperative.[203]

In the early 2010s, dual-use strategies were rather limited. Defence research agencies were driving security-focused R&D, while civilian innovation was led by commercial and academic institutions, with occasional crossover in fields like space and nuclear research. International collaboration in the civil sector was widely encouraged, and research security measures primarily targeted traditional arms control concerns – such as nuclear, chemical, or missile technologies. At the time, emerging fields such as AI, quantum computing, and advanced semiconductors were largely overlooked, in part because they were still in early stages of development and not yet seen as immediate national security risks.[204]

By the mid-2010s, shifting geopolitical dynamics and technological breakthroughs catalysed a strategic shift. Russia's annexation of Crimea in 2014 heightened security concerns in the West, while China's expanding technological ambitions, particularly through Made in China 2025, triggered policy reassessments in many countries[205]. At the same time, AI, autonomous systems, and quantum computing were advancing rapidly – often driven by commercial actors rather than government research. The United States launched the Third Offset Strategy in 2014, leveraging emerging technologies for military applications[206], and soon after, the Defense Innovation Unit (DIU) in 2015, to strengthen ties between the Pentagon and Silicon Valley startups[207]. China institutionalised its Military–Civil Fusion strategy by embedding it in the 13th Five-Year Plan (2016–2020), explicitly directing civilian technological advancements into national defence[208]. In Europe, the UK's 2015 Strategic Defence and Security Review (SDSR) emphasised closer industry collaboration[209], laying the groundwork for initiatives such as the National Security Strategic Investment Fund (NSSIF). Meanwhile, France developed what would later become the Agence de l'Innovation de Défense (AID)[210], and NATO began recognising disruptive technologies as a

[202] Shroff (2020), '"Made in China 2025" Disappears in Name Only'.
[203] Starburst (2023), 'The Rise in Dual-Use Technologies: A Paradigm Shift'; and Baldwin (2024), *Critical Dual-Use Technologies: Commercial, Regulatory, Societal and National Security Challenges*.
[204] Alvarez-Aragones (2024), 'The New Arms Race in Dual-Use Technologies'; and Charatsis (2017), 'Dual-Use Research and Trade Controls: Opportunities and Controversies'.
[205] Shroff (2020), '"Made in China 2025" Disappears in Name Only'.
[206] Pellerin (2016), 'Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence'.
[207] Defense Innovation Unit, 'Who are we/Our mission', available at: https://www.diu.mil/about..
[208] U.S. Department of State (2020), 'The Chinese Communist Party's Military-Civil Fusion Policy'; and Rausch, J. (2021), 'Commercialized Militarization: China's Military-Civil Fusion Strategy'.
[209] UK Government (2015), *National Security Strategy and Strategic Defence and Security Review 2015*.
[210] Ministère des Armées, 'Agence de l'Innovation de Défense', available at: https://www.defense.gouv.fr/aid.

strategic priority, leading to the formation of the NATO Innovation Hub and, in the early 2020s, the DIANA accelerator programme[211].

The past five years have seen an acceleration of policy adaptation in response to global crises. The COVID-19 pandemic exposed vulnerabilities in technology supply chains, while intensifying U.S.-China competition and Russia's 2022 invasion of Ukraine reinforced the urgency of securing critical technologies. Governments have responded by strengthening domestic innovation ecosystems and tightening foreign access to sensitive knowledge. The United States passed the CHIPS and Science Act in 2022, pouring billions into semiconductor manufacturing and R&D, while restricting technology transfers to geopolitical rivals[212]. The EU and Japan followed suit with their own chips acts and investment strategies to reduce reliance on foreign supply chains[213]. New institutional mechanisms also emerged, such as the U.S. Office of Strategic Capital in 2022[214] and Japan's Minister of Economic Security, overseeing technology protection efforts[215]. NATO, recognising the strategic value of emerging technologies, expanded its role with the DIANA accelerator and a EUR 1 billion Innovation Fund in 2023, facilitating transatlantic collaboration in dual-use R&D[216].

As the concept of technological sovereignty gained traction, economic and security policies have become increasingly intertwined. The EU's Economic Security Strategy (2023) and Japan's Economic Security Promotion Act (2022) solidified the idea that protecting critical technologies is as much an economic necessity as a security imperative[217]. Simultaneously, research security measures and export controls have been reinforced, with the EU updating its Dual-Use Regulation in 2021[218] and the U.S., Japan, and Australia tightening frameworks to prevent knowledge leakage and unauthorized technology transfers[219].

This transformation sets the stage for the following sections, where the role of foresight, civil–military innovation integration and research security in shaping modern dual-use R&I strategies is examined in greater detail.

3.2.2. Foresight and civil-military innovation integration

Governments worldwide increasingly recognise that emerging technologies have both economic and security implications, making strategic foresight and well-integrated innovation pipelines essential to dual-use R&I[220]. Anticipatory governance, horizon scanning, and technology roadmaps are now standard tools for identifying and prioritising critical dual-use technologies, ensuring that investments align with long-term security and economic goals[221].

Many countries have formalised processes to guide R&D investments, frequently prioritising AI, semiconductors, quantum computing, biotechnology, space, and advanced communications. These technologies are viewed as transformative for both civilian economies and national security[222]. The rapid advancements in China's technological capabilities have also driven strategic

---

[211] NATO, 'Defence Innovation Accelerator for the North Atlantic', available at: https://www.diana.nato.int/.
[212] PwC (2022), 'The CHIPS Act: What It Means for the Semiconductor Ecosystem'; and U.S. Department of Commerce (2024), 'ICYMI: Secretary Raimondo Delivers Update on CHIPS and Science Act Implementation, Lays Road Ahead for Supercharging Innovation and Revitalizing American Semiconductor Manufacturing'.
[213] European Commission (2024), European Chips Act; and Government of Japan (2024), 'Strengthening Collaboration Between Japan and the Republic of Korea in Advanced Science and Technology'.
[214] U. S. Department of Defense, 'Office of Strategic Capital', available at: https://www.cto.mil/osc/.
[215] Osawa (2023), 'How Japan Defines Economic Security'.
[216] KARVE (2023), 'UK Defence Innovation Funds & Accelerator Programmes'; and O'Dwyer (2024), 'Finland to Host NATO Tech Centers, Revamp Cybersecurity Strategy'.
[217] Osawa (2023), 'How Japan Defines Economic Security; and Pannier (2023), 'Balancing Security and Openness for Critical Technologies: Challenges for French and European Research'.
[218] Commission Recommendation (EU) 2021/1700.
[219] Hudson (2024), 'How Will the New US Research Security Centre Work?'.
[220] Starburst (2023), 'The Rise in Dual-Use Technologies: A Paradigm Shift'.
[221] Kolliarakis (2022), 'Anticipatory Governance of Emerging and Disruptive Technologies with Dual-Use Potential'.
[222] European Commission (2024), *White Paper on options for enhancing support for research and development involving technologies with dual-use potential*.

adjustments in the U.S., Europe, and allied nations, with a growing emphasis on securing domestic innovation ecosystems[223].

At the core of this strategic shift is a stronger linkage between civilian and defence innovation. Given that commercial enterprises now drive many technological breakthroughs, governments have increasingly adopted so-called 'spin-in' models — bringing civilian innovations into defence use. At the same time, 'spin-offs' aim to transfer defence-funded research to civilian markets, ensuring two-way benefits. In Japan, for example, mechanisms to support such bidirectional flow have been institutionalised through a dual-use defence startup ecosystem[224]. Several mechanisms support this bidirectional flow:

- *Public-private partnerships***:** Many nations have promoted joint R&D initiatives where defence agencies collaborate with the industry to accelerate dual-use innovation. The U.S. Defense Innovation Unit (DIU) exemplifies this model, connecting Silicon Valley startups with military needs[225]. The UK's Defence and Security Accelerator (DASA) plays a similar role, as does NATO's new DIANA, which fosters startup-driven defence solutions across allied nations[226]. However, recent studies suggest these partnerships often fall short of their potential. Ministries of defence frequently lack the mechanisms to engage non-traditional players or systematically leverage dual-use technologies, despite strong stated intentions[227]. Effective implementation – not the number of partnerships – appears to be the key constraint.[228]
- *Targeted funding and venture capital:* Recognising that startups and small firms often spearhead innovation, governments are starting to introduce dedicated investment mechanisms. The U.S. SBIR (Small Business Innovation Research) programme allocates federal R&D funds to small companies for defence-relevant innovation[229]. Similar initiatives include Poland's EUR 100 million Defence Fund, NATO's Innovation Fund, and Israel's INNOFENSE incubator, all of which help commercial firms develop dual-use applications[230]. However, despite these promising initiatives, many Ministries of Defence continue to rely heavily on traditional prime contractors, with limited mechanisms to engage startups and non-traditional actors – a gap frequently cited as a barrier to defence innovation[231].
- *Innovation hubs and accelerators:* Fast-tracking civilian technologies for defence applications has become a strategic priority. Governments are setting up dedicated innovation hubs to scout and integrate private-sector innovations into defence. The U.S. Office of Strategic Capital and Japan's Minister of Economic Security aim to mobilize private investment into strategic technologies while safeguarding critical know-how[232].
- *Spin-off programmes and tech transfer offices:* To ensure that defence-funded research finds broader commercial applications, institutions like NASA and national defence R&D agencies manage structured technology transfer programmes. These "spin-off" pathways help civilianise military-developed innovations – from satellite technologies to

[223] Gallo (2025), 'The Defense Innovation Ecosystem'.
[224] Kousuke (2024), 'Japan's Push for a Dual-Use Defence Startup Ecosystem'.
[225] Madsen (2020), 'Defence Innovation Unit SBIR/STTR'; and Laje (2024), 'Small Businesses Adapt for Advantage in Dual-Use Era'.
[226] KARVE (2023), 'UK Defence Innovation Funds & Accelerator Programmes'; and NATO, 'Defence Innovation Accelerator for the North Atlantic'.
[227] CESAER (2024), 'Strengthen Dual-Use Technologies by Enhancing EU Defence Funding'; and Laje (2024), 'Small Businesses Adapt for Advantage in Dual-Use Era'.
[228] Schlueter et al. (2025), 'Overcoming the Six Unspoken Barriers That Impede Defense Innovation'.
[229] Madsen (2020), 'Defence Innovation Unit SBIR/STTR'; and Laje (2024), 'Small Businesses Adapt for Advantage in Dual-Use Era'.
[230] Lawrence (2024), 'Polish startups set to benefit from new €100M Defence Fund'; CESAER (2024), 'Strengthen Dual-Use Technologies by Enhancing EU Defence Funding'; and Greenberg (2025), 'Israel creates hub to hasten military AI, autonomy research'.
[231] Schlueter et al. (2025), 'Overcoming the Six Unspoken Barriers That Impede Defense Innovation'.
[232] U. S. Department of Defense, 'Office of Strategic Capital'; Osawa, J. (2023), 'How Japan Defines Economic Security'; and Government of Japan (2024), 'Strengthening Collaboration Between Japan and the Republic of Korea in Advanced Science and Technology'.

cybersecurity tools – ensuring public value[233]. In Europe, national defence research agencies oversee tech transfer efforts, while spin-in schemes such as the European Defence Fund's EUDIS initiative support the reverse flow: integrating commercial technologies into defence use[234].

With private-sector R&D outpacing government-led defence research in key areas such as AI, biotech, and quantum computing, militaries are increasingly leveraging commercial technologies rather than developing them in isolation. However, balancing open innovation with security remains a challenge. Governments are tightening research security frameworks, reinforcing intellectual property protections, and selectively restricting foreign access to sensitive technologies to prevent adversarial exploitation.

3.2.3. Research security and responsible internationalisation

As governments expand dual-use R&I strategies, balancing open scientific collaboration with national security concerns has become a core challenge. Increasing geopolitical competition has led many countries to adopt research security frameworks to safeguard critical knowledge, while also promoting responsible internationalisation to ensure that global R&D cooperation remains both open and secure. Governments increasingly acknowledge that these two approaches must be complementary rather than contradictory. By combining regulatory safeguards with proactive risk management tools, countries aim to sustain international scientific collaboration while ensuring that sensitive research remains protected.[235]

- *Intellectual property protection:* Many governments have introduced stricter measures to prevent unauthorised technology transfers. Japan's Economic Security Promotion Act (2022) requires national security reviews for patent applications, restricting disclosure of strategically sensitive innovations[236]. Germany's research security guidelines encourage institutions to classify and protect sensitive knowledge, limiting access where needed[237]. The EU's Horizon Europe (HE) and European Defence Fund (EDF) have introduced clearer IPR provisions to protect sensitive results and ensure commercial viability within their respective mandates[238]. However, both programmes are bound by legal constraints that limit their scope to exclusively civil (HE) or exclusively defence (EDF) applications. As such, neither is currently designed to support integrated dual-use R&D projects.[239]
- *Foreign research influence and investment screening:* The U.S. Committee on Foreign Investment (CFIUS) has expanded its remit to cover strategic tech acquisitions[240], while the UK's National Security and Investment Act grants the government authority to block investments in critical sectors[241]. The EU's foreign direct investment (FDI) screening framework is used to prevent hostile takeovers of high-tech firms[242]. Universities in several

[233] CESAER (2024), 'Strengthen Dual-Use Technologies by Enhancing EU Defence Funding'.
[234] European Commission (2025), 'European Defence Fund: Over €1 Billion to Drive Next-Generation Defence Technologies and Innovation'; and European Commission, EUDIS, available at: https://eudis.europa.eu/index_en.
[235] CESAER (2024), 'Strengthen Dual-Use Technologies by Enhancing EU Defence Funding'.
[236] Osawa (2023), 'How Japan Defines Economic Security'.
[237] Federal Ministry of Education and Research (2024), 'Position Paper of the German Federal Ministry of Education and Research on Research Security in Light of the Zeitenwende'.
[238] Blasi (2024), *Horizon Europe: Protecting academic freedom – Strengthening and improving implementation of Recital 72*; and European Commission (2025), 'European Defence Fund: Over €1 Billion to Drive Next-Generation Defence Technologies and Innovation'.
[239] CESAER (2024), 'Strengthen Dual-Use Technologies by Enhancing EU Defence Funding'.
[240] Linney, Cook, and Jansen (2025), 'CFIUS Has Circled Its Civil Enforcement Wagons — Trump 2.0 Is Likely to Build upon Activities Begun by Biden Administration'.
[241] UK Government (2024), 'National Security and Investment Act: guidance for the higher education and research-intensive sectors'.
[242] Kauppila, and Cappelin (2023), 'The China Dilemma in Foreign Direct Investment Screening: Comparing the Finnish and Swedish Approaches'.

countries are also required to conduct due diligence on international partnerships to ensure that collaborations do not inadvertently benefit strategic competitors[243].

- *Export controls and compliance:* Export controls are increasingly shaping the boundaries of international research and innovation. In the United States, the Export Administration Regulations (EAR) – which apply to dual-use technologies – have been expanded to cover AI software, quantum encryption, and advanced semiconductors, while certain defence-related items remain under the International Traffic in Arms Regulations (ITAR)[244]. In the EU, the 2021 update to the Dual-Use Regulation clarified that academic and research institutions are subject to the same due diligence obligations as industry actors. While the requirement for export licences in sensitive collaborations already existed under Regulation 428/2009, the revised regulation introduced new transparency mechanisms and additional controls on cyber-surveillance technologies.[245].
- *Cybersecurity and counter-espionage measures:* Research institutions are strengthening internal systems to counter cyber threats, data theft, and foreign interference. Finland has pioneered secure data enclaves for sensitive research[246], while the UK's National Cyber Security Centre (NCSC) and the U.S. National Science Foundation (NSF) have issued guidelines for universities handling dual-use technologies. NSF's TRUST framework and Australia's UFIT guidelines both combine disclosure procedures with institutional risk management tools and training, serving as models for collaborative, compliance-driven approaches[247].

Rather than restricting global research cooperation entirely, many countries have introduced frameworks to help national actors engage internationally while managing security risks. Three common approaches can be identified:

- *National guidelines and risk assessment tools:* Several governments have issued national-level guidance to help researchers and institutions navigate sensitive partnerships. Canada's National Security Guidelines for Research Partnerships (NSGRP) require documented risk assessments for certain international collaborations[248]. Sweden has drafted similar guidance and have drafted a proposal for a support structure[249], while the UK's Trusted Research initiative provides practical checklists to assess the trustworthiness of partners and projects[250]. OECD has also promoted trusted research frameworks to support a balance between openness and protection[251].
- *Institutional protocols and compliance requirements:* A growing number of funding agencies require research-performing organisations to adopt internal processes for managing security risks. In the U.S., the NSF's TRUST framework and Secure Research Ecosystem call for universities to implement disclosure procedures, compliance systems,

[243] Longfield (2024), *The Security of Research Partnerships Between Canadian Universities, Research Institutions and Entities Connected to the People's Republic of China*.
[244] Charatsis (2017), 'Dual-Use Research and Trade Controls: Opportunities and Controversies'; and JASON advisory group (2024), *Safeguarding the Research Enterprise*.
[245] JASON advisory group (2024), *Safeguarding the Research Enterprise*.
[246] O'Dwyer (2024), 'Finland to Host NATO Tech Centers, Revamp Cybersecurity Strategy'; and Prime Minister's Office of Finland (2024), *Finland's Cyber Security Strategy 2024–2035*.
[247] Australian Government (2021), 'Guidelines to Counter Foreign Interference in the Australian University Sector'; U.S. National Science Foundation (2024), 'Trusted Research Using Safeguards and Transparency (TRUST)'; and Hudson (2024), 'How Will the New US Research Security Centre Work?'.
[248] U15 Canada (2023), 'Safeguarding Research in Canada: A Guide for University Policies and Practices'; and Innovation, Science and Economic Development Canada (2023), 'National Security Guidelines for Research Partnerships'.
[249] Swedish Council for Higher Education, Swedish Research Council, and Vinnova (2024), *Responsible Internationalisation – Interim Report on a Government Assignment 2024*; and Swedish Council for Higher Education, Swedish Research Council, and Vinnova (2024), *National Support Function for Responsible Internationalisation – Final Report 2025*.
[250] National Protective Security Authority (2024), 'Trusted Research Guidance for Academics'.
[251] OECD (2023), *OECD Science, Technology and Innovation Outlook 2023: Enabling Transitions in Times of Disruption*.

and foreign influence mitigation strategies as conditions for funding[252]. Australia's UFIT guidelines are similarly embedded in ARC grant requirements[253], while the UK's National Protective Security Authority (NPSA) provides institutional guidance to manage risks in foreign collaborations[254].

- *Training, coordination, and cross-agency support structures:* Countries such as Canada, Germany, and Australia have introduced structured training modules for researchers and administrators[255]. Coordination platforms such as Australia's UFIT and the U.S. Academic Security and Counter Exploitation (ASCE) Program facilitate information sharing between universities, government agencies, and national security services[256]. Sweden is also exploring cross-functional models through its proposed pilot support function for responsible internationalisation[257].

In parallel, the EU has introduced a series of initiatives to address research security and responsible internationalisation. As part of its 2024 Economic Security Package, the Commission proposed a Council Recommendation on Research Security and launched a White Paper on R&D support for dual-use technologies[258]. Additional tools include a foreign interference mitigation toolkit for universities and Horizon Europe safeguards to control participation and knowledge flows[259]. These measures underscore the EU's growing attention to research risks and provide important context for comparing how international actors are approaching similar challenges[260].

3.3. International Case Studies

This section applies the three-dimensional analytical framework to explore how key countries and regions have developed strategic approaches to dual-use R&I. The case studies illustrate how national systems balance long-term technology prioritisation, civil–defence innovation flows, and research security in practice. Each case reflects a distinct configuration of foresight mechanisms, tech transfer tools, and risk mitigation policies – shaped by geopolitical context, governance structures, and institutional capabilities.

Rather than offering one-size-fits-all models, the case studies highlight the diversity of national responses and allow for comparative insights. The analysis draws on national strategies, implementation programmes, and institutional practices, following a consistent structure across countries to facilitate benchmarking. Taken together, they provide an empirical foundation for the strategic observations that follow in section 3.4.

3.3.1. North America

United States: global leader in dual-use R&I integration

The U.S. has one of the most mature dual-use R&I ecosystems, characterized by strong foresight, robust civilian–defence innovation interfaces, and structured funding mechanisms. Unlike more

[252] U.S. National Science Foundation (2024), 'Trusted Research Using Safeguards and Transparency (TRUST).
[253] Australian Government (2021), 'Guidelines to Counter Foreign Interference in the Australian University Sector'.
[254] National Protective Security Authority (2024), 'Trusted Research Guidance for Senior Leaders'.
[255] U15 Canada (2023), 'Safeguarding Research in Canada: A Guide for University Policies and Practices'; Federal Ministry of Education and Research (2024), 'Position Paper of the German Federal Ministry of Education and Research on Research Security in Light of the Zeitenwende'; and Australian Government (2021), 'Guidelines to Counter Foreign Interference in the Australian University Sector'.
[256] Australian Government (2021), 'Guidelines to Counter Foreign Interference in the Australian University Sector'; Research and Innovation Security and Competitiveness Institute, 'Programs and Partners', https://risc.tamus.edu/.
[257] Swedish Council for Higher Education, Swedish Research Council, and Vinnova (2024), *National Support Function for Responsible Internationalisation – Final Report 2025*.
[258] European Commission (2024), *Proposal for a Council Recommendation on enhancing research security*; SwissCore (2024), 'Commission Adopts Economic Security Package'; and European Commission (2024), *White Paper on options for enhancing support for research and development involving technologies with dual-use potential*.
[259] European Commission (2022), 'Tackling R&I foreign interference'.
[260] European Commission, 'Strategic Autonomy and European Economic and Research Security'.

centralised models such as China's, the U.S. approach relies on distributed innovation actors and mission-oriented agencies to link civilian and military technology development. The Department of Defense (DoD) sets strategic priorities through national roadmaps, such as the National Defense Science & Technology Strategy, focusing on AI, quantum, hypersonics, and space[261]. Agencies like DARPA drive high-risk, high-reward innovation[262], while broader initiatives like the CHIPS and Science Act ensure long-term investments in critical technologies[263]. Mechanisms like the Defense Innovation Unit (DIU) and the SBIR (Small Business Innovation Research) and STTR (Small Business Technology Transfer) programs bridge the gap between commercial startups and defence needs – accelerating tech transfer and reducing procurement barriers[264]. While SBIR focuses on early-stage funding for small businesses, STTR specifically supports collaborations between small firms and research institutions.

The innovation pipeline is reinforced through venture capital engagement, rapid acquisition reforms, and targeted co-investments by agencies like In-Q-Tel[265] and the Office of Strategic Capital[266]. Hackathons, prize competitions, and flexible contracting mechanisms help fast-track emerging technologies into military applications. The U.S. has also expanded partnerships with industry through initiatives like AFWERX[267] and xTechSearch[268], ensuring that civilian tech developments contribute directly to defence capabilities. At the same time, structural challenges persist – including fragmented acquisition pathways, financial barriers for small firms, and the need for "trilingual" leadership that can bridge operational, technical, and procurement communities[269]. Addressing these gaps has been central to recent innovation efforts, which emphasise agile contracting, end-user involvement, and leadership commitment as key success factors[270]. The continuity of this model reflects longstanding patterns of trust-based collaboration between government, academia, and private capital – a dynamic first institutionalised in the Cold War-era emergence of Silicon Valley as a dual-use innovation hub, and repeatedly adapted to meet evolving technological and strategic demands.[271]

Research security has become a priority, balancing openness with national security concerns. Policies such as NSPM-33 enforce disclosure requirements for foreign ties in federally funded research, while export controls and investment screenings restrict sensitive tech from adversarial access[272]. The U.S. actively coordinates security measures with allies through mechanisms like the Wassenaar Arrangement[273] and G7 technology governance initiatives[274]. The NSF's TRUST framework further supports institutional compliance through structured disclosure rules, training, and shared responsibility models[275]. While these restrictions aim to protect national interests, efforts are made to sustain international collaboration in key scientific domains – for example,

[261] Madsen (2020), 'Defence Innovation Unit SBIR/STTR'.
[262] Defense Advanced Research Projects Agency, 'About DARPA', available at: https://www.darpa.mil/about.
[263] Van Hollen's office in the US Senate (2022), 'CHIPS and Science Act of 2022 Division A Summary - CHIPS and ORAN Investment'.
[264] Laje (2024), 'Small Businesses Adapt for Advantage in Dual-Use Era'.
[265] IQT, 'Homepage', available at: https://www.iqt.org/.
[266] U.S. Department of Defense, 'Office of Strategic Capital', available at: https://www.cto.mil/osc/.
[267] AFWERX – Accelerating Agile Innovation for the U.S. Air Force, available at: https://afwerx.com/.
[268] XTech, available at: https://xtech.army.mil/.
[269] Starburst (2023), 'The Rise in Dual-Use Technologies: A Paradigm Shift'.
[270] Laje (2024), 'Small Businesses Adapt for Advantage in Dual-Use Era'.
[271] Steve Blank Secret History, available at: https://steveblank.com/secret-history/.
[272] U.S. National Science Foundation (2024), 'NSF-Backed SECURE Center Will Support Research Security, International Collaboration'; and U.S. National Science Foundation, 'Research Security at the National Science Foundation'.
[273] Wassenaar Arrangement Secretariat, 'The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies'.
[274] CESAER (2023), 'Workshop on Research Security – GSF-01 Multilateral Dialogue on Principles and Values in International Research & Innovation Cooperation', pp.13-20.
[275] U.S. National Science Foundation (2024), 'Trusted Research Using Safeguards and Transparency (TRUST)'.

through Five Eyes science partnerships[276], U.S.–EU digital policy dialogues[277], and trusted research exchanges with countries like the UK[278] and Japan[279].

3.3.2. Asia-Pacific

China: state-driven dual-use strategy through military-civil fusion

China's dual-use R&I strategy is highly centralised, with the state coordinating innovation efforts under the Military-Civil Fusion (MCF) policy – a strategic initiative aimed at erasing barriers between the civilian and military science and technology ecosystems[280]. National plans such as Made in China 2025 and successive Five-Year Plans set clear priorities, emphasising AI, quantum, hypersonics, and advanced manufacturing as key to both economic and military dominance. Massive state funding and industrial policy instruments drive these efforts, integrating military needs into broader technological development[281]. The People's Liberation Army (PLA) actively collaborates with civilian universities and private firms through MCF committees, ensuring that technology flows efficiently between sectors – often via institutions with strong defence ties, such as the so-called "Seven Sons" universities[282]. Despite its ambitions, MCF faces challenges – including fragmented implementation at local levels, institutional silos between civil and defence actors, and increasing international scrutiny[283]. Several Chinese entities and affiliated research institutions have been subject to export restrictions, and global partnerships have come under pressure due to concerns over military end-use and the opacity of China's MCF system[284].

China's innovation pipeline is supported by major state-owned enterprises and private tech firms that engage in defence projects under government direction[285]. Companies like Huawei, DJI, and Baidu have been linked to military programmes through partnerships with PLA-affiliated institutions and participation in state-led dual-use initiatives[286]. Large-scale procurement mechanisms, industrial espionage, and forced tech transfers complement these efforts, ensuring rapid adoption of emerging technologies[287]. Leveraging its vast domestic market, China achieves economies of scale in critical areas such as drones and semiconductor fabrication, reinforcing its technological self-sufficiency[288].

Research security in China is strict with laws like the National Security Law and Data Security Law tightly controlling knowledge flows. Scholars and institutions require government approval for international collaboration, and outbound technology transfers are heavily regulated[289]. Simultaneously, China actively acquires foreign tech through investment, talent recruitment, and cyber operations[290]. Recent Western countermeasures, such as the U.S. export controls on

[276] Cueto (2024), 'Five Eyes International Intelligence Alliance Launches Collaborative Security Initiative'.
[277] Burwell (2024), 'Looking ahead to the next chapter of US-EU digital collaboration'.
[278] U.S. Department of Commerce (2024), 'U.S. and UK Announce Partnership on Science of AI Safety'.
[279] Henry (2024), 'US, Japan to Conduct Research Exchanges on Emerging Tech'.
[280] U.S. Department of State (2020), 'The Chinese Communist Party's Military-Civil Fusion Policy'.
[281] Rausch (2021), 'Commercialized Militarization: China's Military-Civil Fusion Strategy'.
[282] U.S. Department of State (2020), 'The Chinese Communist Party's Military-Civil Fusion Policy'.
[283] Mc Nicholas (2024), 'China's Military-Civil Defusion'.
[284] Kelly, and Qian (2025), 'U.S. and China Just Set New Road Rules for Science Collaboration. Americans Will Benefit If We Don't Scrap Joint Research'.
[285] Rausch (2021), 'Commercialized Militarization: China's Military-Civil Fusion Strategy'.
[286] Joshi (2022), 'China's Military-Civil Fusion Strategy, the US Response, and Implications for India'; and U.S. Department of State (2020), 'The Chinese Communist Party's Military-Civil Fusion Policy'.
[287] Farrow (2023), 'Modernization and the Military-Civil Fusion Strategy'.
[288] Atkinson (2024), 'China Is Rapidly Becoming a Leading Innovator in Advanced Industries'.
[289] Arcesati, Ghiretti, and Schwaag Serger (2023), 'In Research Collaboration, Drawing Red Lines with China Isn't Easy'; and CESAER (2023), 'Workshop on Research Security – GSF-01 Multilateral Dialogue on Principles and Values in International Research & Innovation Cooperation'.
[290] CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper'.

semiconductors, have prompted China to accelerate indigenous innovation, further reinforcing its drive for technological self-reliance[291].

Japan: strategic shift toward dual-use R&I through economic security

Japan has traditionally maintained a separation between civilian and defence R&D, but recent geopolitical tensions have pushed it toward a more integrated dual-use strategy[292]. The Economic Security Promotion Act (2022) introduced measures to secure critical technologies, funding R&D in AI, quantum, and semiconductors while enhancing regulatory oversight[293]. The Science and Technology Basic Plans now include explicit security considerations, and Japan has deepened cooperation with allies through initiatives such as AUKUS working groups and a fighter jet co-development project with the UK and Italy[294].

Japan's innovation pipeline is shifting to leverage its strong commercial tech base for defence applications[295]. The government incentivizes dual-use development through programmes like ATLA's grants for civilian labs researching metamaterials and AI[296]. Major industrial players, such as Mitsubishi and Toshiba, are increasingly encouraged to align their research with national security priorities[297]. Space technology is a key focus, with JAXA collaborating closely with the Ministry of Defence on surveillance and communication satellites[298]. Japan's more recent "K-Program" also supports dual-use innovation through competitive grants, though the initiative has faced challenges due to security clearance requirements that limit participation from some academic institutions[299].

Research security measures have tightened, with Japan expanding export controls and introducing a patent non-disclosure system to prevent sensitive discoveries from reaching foreign adversaries. Visa screening for foreign students in critical fields has been enhanced and select collaborations with Chinese institutions have been curtailed. Japan has also aligned more closely with the U.S. on semiconductor restrictions, limiting the transfer of advanced manufacturing technologies to China.

Republic of Korea: balancing commercial technological leadership with strategic dual-use innovation

Republic of Korea has gradually shifted from a commercial tech-driven approach to a dual-use strategy focused on defence modernisation and economic security[300]. Government foresight has identified AI, aerospace, semiconductors, and cybersecurity as priority areas, reflected in strategic initiatives like the Defence Innovation Committee and Science & Technology Basic Plans[301]. Military modernisation efforts emphasize integrating Fourth Industrial Revolution technologies, with plans to develop AI-driven surveillance, robotics, and space capabilities[302].

Republic of Korea's innovation pipeline benefits from its world-class industrial giants, such as Samsung and Hanwha, which operate in both civilian and military markets[303]. The Defence

[291] Sutter, and Sutherland (2021), 'China's 14th Five-Year Plan: A First Look'.
[292] Kousuke (2024), 'Japan's Push for a Dual-Use Defence Startup Ecosystem'; and 村山 裕三 Murayama, Yuuzou (2020), '国家安全保障と経済の両立に向けた技術戦略 (Technology Strategy for Balancing National Security and the Economy)'.
[293] Osawa (2023), 'How Japan Defines Economic Security'; Colecchia (2025), 'OECD STI Outlook 2025 (Work in Progress): International Cooperation and Competition in Science and Technology and the Geopolitical Context'.
[294] Henry (2024), 'US, Japan to Conduct Research Exchanges on Emerging Tech'.
[295] Kousuke (2024), 'Japan's Push for a Dual-Use Defence Startup Ecosystem'.
[296] Osawa (2023), 'How Japan Defines Economic Security'.
[297] Kousuke (2024), 'Japan's Push for a Dual-Use Defence Startup Ecosystem'.
[298] Ministry of Defence of Japan (2019), 'Defense of Japan 2019 – Section 4-2-2: Initiatives in the Space Domain'.
[299] Colecchia (2025), 'OECD STI Outlook 2025 (Work in Progress): International Cooperation and Competition in Science and Technology and the Geopolitical Context'.
[300] Wooyeal (2024), 'South Korean Defense Industry Goes Global, and Local Too: An Econo-Tech Approach'.
[301] Ramage (2024) 'Timeline of the South Korean Government's AI Efforts'.
[302] Yoon (2023), 'Emerging New Military Technologies in Northeast Asia and Implications for South Korean Defense Strategy'.
[303] Wooyeal (2024), 'South Korean Defense Industry Goes Global, and Local Too: An Econo-Tech Approach'.

Acquisition Program Administration (DAPA) promotes tech transfer by inviting commercial startups to develop military applications[304]. International cooperation, particularly with the U.S., plays a major role, as seen in joint R&D programs on quantum computing and biotech[305]. Republic of Korea also contributes to NATO innovation funds, ensuring access to global dual-use collaborations[306].

Research security has become a focus, particularly in managing economic ties with China while adhering to Western security frameworks[307]. The government has strengthened regulations on foreign investment in strategic sectors and enhanced screening of Chinese students in sensitive fields[308]. The National Core Technology list imposes strict transfer restrictions, and enforcement has been intensified to protect semiconductor and defence-related IP[309]. Cybersecurity efforts have also been bolstered, with private-sector collaboration to secure critical infrastructure[310].

3.3.3. Middle East

Israel: a highly integrated dual-use innovation ecosystem

Israel has made significant efforts to connect its dynamic civilian tech sector with national security objectives, with policy frameworks prioritising cybersecurity, AI, unmanned systems, and advanced communications[311]. Defence units like Unit 8200 have long acted as talent incubators for the startup ecosystem, while public programmes such as INNOFENSE promote the adaptation of commercial technologies for defence purposes[312]. The Ministry of Defence and the Israel Innovation Authority jointly fund early-stage dual-use innovation[313]. However, recent critiques – particularly after the events of October 7 – have pointed to challenges in translating these innovations into battlefield-ready capabilities, highlighting coordination gaps between Israel's startup sector and its operational defence needs[314].

Israel's innovation pipeline is structured to support dual flows between defence and civilian applications[315]. The Israeli Defense Forces (IDF) engage directly with startups and industry actors to accelerate the development and adoption of emerging technologies – particularly in areas such as AI-enabled surveillance and battlefield robotics[316]. Military-backed incubators provide early-stage funding and mentorship, supporting firms like Check Point, Elbit Systems, and NSO Group that have expanded into global cybersecurity and defence markets[317]. At the same time, leading universities such as the Technion and Tel Aviv University contribute to the defence innovation base by spinning off deep-tech startups and aligning research with military R&D programmes[318].

---

[304] Defense Acquisition Program Administration, available at: https://www.dapa.go.kr/dapa_en/main.do.

[305] Science and Technology Policy Institute (2024). '국방 혁신과 듀얼유즈 전략: 산업계 참여 확대를 위한 정책방향 [Defense Innovation and the Dual-Use Strategy: Industrial Participation and Policy Recommendations]'.

[306] CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper'.

[307] CESAER (2023), 'Workshop on Research Security – GSF-01 Multilateral Dialogue on Principles and Values in International Research & Innovation Cooperation'.

[308] Ramage (2024) 'Timeline of the South Korean Government's AI Efforts'.

[309] Korea Industry Daily (2023). '반도체·방산기술 해외 유출시 최대 징역 15년 [Up to 15 Years Imprisonment for Overseas Leakage of Semiconductor and Defense Technology]'.

[310] Strouse et al. (2023), *Safeguarding International Science: Research Security Framework*.

[311] Greenberg (2025), 'Israel creates hub to hasten military AI, autonomy research'.

[312] Frantzman (2023), 'How Israel's military is prioritizing dual-use start-ups to accelerate defense tech'.

[313] Israel Ministry of Defence, 'Military Research and Development'.

[314] Israel Innovation Authority (2024), 'A Year Since October 7: A Situation Report on the Israeli High-Tech Sector'.

[315] Greenberg (2025), 'Israel creates hub to hasten military AI, autonomy research'.

[316] Frantzman (2023), 'How Israel's military is prioritizing dual-use start-ups to accelerate defense tech'.

[317] Wikipedia, 'Israeli Cybersecurity Industry'; Marcucci (2024), 'From Lasers to Lavender: Will Israel's Dual-Use Technology Lead To Dual-Use Societies?'.

[318] Getz et al., 'בינה מלאכותית, מדעי הנתונים ורובוטיקה חכמה – דו"ח ראשון" (Artificial Intelligence, Data Science, and Smart Robotics – First Report)'; and Deloitte Corporate Finance Israel (2024), 'Israel Cyber Industry Overview'.

While Israel is deeply integrated into global innovation networks, it enforces strict research security measures. The Defense Export Controls Agency (DECA) tightly regulates technology transfers, ensuring that sensitive dual-use innovations remain under national oversight[319]. Concerns over foreign influence have led to increased scrutiny of Chinese investments, with a 2019 foreign investment review committee curbing foreign control in critical high-tech sectors[320]. Cybersecurity remains a top priority, with the Israel National Cyber Directorate coordinating resilience efforts across government, academia, and industry[321]. Through strong ties with the U.S. and European allies, Israel continues to leverage joint R&D while safeguarding its technological edge[322].

3.3.4. Europe

Germany: strengthening dual-use R&I in response to geopolitical shifts

Germany's approach to dual-use R&I has undergone a shift, particularly following its *Zeitenwende* (turning point) in 2022. Historically, Germany maintained a conservative defence R&D stance, relying on civilian innovation to feed into military needs. However, the establishment of SPRIND (Federal Agency for Disruptive Innovation) in 2019 signalled a move toward a DARPA-like model, fostering high-risk, high-reward research with dual-use applications. Germany's High-Tech Strategy prioritizes AI, quantum computing, and cybersecurity, aligning with both industrial and defence interests[323]. The country also increasingly coordinates its foresight efforts with NATO and EU initiatives[324], contributing to major European defence projects such as the FCAS (Future Combat Air System) and the Main Ground Combat System[325].

Germany's industrial base plays a key role in bridging civil and military applications. Companies like Siemens, Bosch, and BMW innovate across both domains, with developments in automation, advanced materials, and electronics benefiting both commercial and defence applications[326]. The Cyber Innovation Hub of the Bundeswehr serves as an incubator for startups, helping civilian tech firms adapt their solutions to security and defence needs[327]. Moreover, Germany is among the strongest contributors to NATO's Innovation Fund, ensuring that European dual-use startups gain access to venture capital[328]. Germany has also been leveraging defence procurement to drive tech transfer, negotiating technology-sharing commitments when acquiring foreign military systems[329].

On research security, Germany has recently tightened regulations to safeguard sensitive technologies. The BMBF (Ministry of Education and Research) published a Research Security Position Paper in 2024, calling for universities to implement risk assessment tools and security

[319] Israel Ministry of Defence, 'DECA: Defense Export Control Agency'.
[320] TheMarker (2024), 'ישראל משנה גישה: טכנולוגיה אזרחית תחת פיקוח בטחוני [Israel Shifts Approach: Civilian Tech Under Security Oversight]'.
[321] Deloitte Corporate Finance Israel (2024), 'Israel Cyber Industry Overview'; and YL Ventures (2025), 'The State of the Cyber Nation 2024'.
[322] Greenberg (2025), 'Israel creates hub to hasten military AI, autonomy research'.
[323] Federal Ministry of Education and Research (2024), 'Position Paper of the German Federal Ministry of Education and Research on Research Security in Light of the Zeitenwende'; and Barker, and Hagebölling (2022), 'A German Digital Grand Strategy: Integrating Digital Technology, Economic Competitiveness, and National Security in Times of Geopolitical Change'.
[324] Arcesati, Ghiretti, and Schwaag Serger (2023), 'In Research Collaboration, Drawing Red Lines with China Isn't Easy'; and Niinistö (2024), *Safer Together – Strengthening Europe's civilian and military preparedness and readiness*.
[325] Deutscher Bundestag (2024), 'Pläne der Bundesregierung zur Forschungssicherheit im Lichte der Zeitenwende'.
[326] Barker, and Hagebölling, (2022), 'A German Digital Grand Strategy: Integrating Digital Technology, Economic Competitiveness, and National Security in Times of Geopolitical Change'; and Barker, and Hagebölling (2022), 'Deutschlands wirtschaftliche Sicherheit und Technologie'.
[327] SPD-Bundestagsfraktion (2024), 'Stärkung Der Sicherheits- Und Verteidigungsindustrie in Deutschland Und Europa'.
[328] Starburst (2023), 'The Rise in Dual-Use Technologies: A Paradigm Shift'.
[329] SPD-Bundestagsfraktion (2024), 'Stärkung Der Sicherheits- Und Verteidigungsindustrie in Deutschland Und Europa'.

vetting in international collaborations[330]. The German Academic Exchange Service's (DAAD) KIWi (Knowledge Integrity and Security Initiative) provides guidelines on cybersecurity, due diligence, and IP protection, reflecting Germany's growing concern over foreign technology leakage[331]. Meanwhile, Germany has amended its export control laws and strengthened investment screening, blocking several Chinese acquisition attempts in semiconductors and AI-driven automation[332]. These measures reflect Germany's evolving balance between innovation openness and national security considerations.

France: Strategic autonomy and dual-use R&I for technological sovereignty

France's dual-use R&I strategy is deeply embedded in its broader push for strategic autonomy, ensuring national and European leadership in critical technologies. The Agence de l'Innovation de Défense (AID), established in 2018, coordinates foresight efforts, identifying AI, robotics, cyber-defence, and space as priority areas. These align with France's broader national industrial strategies, such as its AI roadmap, which integrates civil and military applications[333]. France's investment in supercomputing and quantum technology – backed by over €500 million in dedicated defence and recovery funding since 2020 – reflects its ambition to lead in dual-use digital innovation[334].

France's dual-use innovation ecosystem is driven by strong public-private collaboration. Major defence firms such as Thales, Airbus, and Dassault operate across civilian and military sectors, ensuring cross-pollination of technologies. Airbus, for example, develops aeronautical innovations that benefit both commercial and defence aviation. The government supports this ecosystem through programmes like DefInvest, a €50 million investment fund launched in 2018 to support dual-use startups, and through joint innovation hubs such as the Pôles d'Innovation, where civilian and military R&D efforts intersect[335]. While modest in size compared to U.S. SBIR/STTR schemes, these efforts reflect France's broader ambition to align sovereign tech development with national defence needs. At the European level, France plays a central role in flagship defence projects such as FCAS (Future Combat Air System) and next-generation European encryption technologies, reinforcing the European strategic autonomy agenda[336].

In terms of research security and internationalisation, France has tightened oversight in recent years. While traditionally more open than the U.S. or UK, concerns over foreign influence in strategic sectors have led to increased scrutiny of academic partnerships, particularly with China and Russia. Universities now consult with security authorities before engaging in high-risk collaborations[337]. France enforces strict export controls, particularly on cyber tools, and has aligned with the EU's new foreign investment screening mechanisms. In defence R&D, France emphasizes European sovereignty, actively seeking alternatives to reliance on U.S. or Chinese technologies in emerging fields like AI and semiconductors[338].

---

[330] Federal Ministry of Education and Research (2024), 'Position Paper of the German Federal Ministry of Education and Research on Research Security in Light of the Zeitenwende'; and Rat für technologische Souveränität (2024), 'Schlüsseltechnologien im Fokus – Der Wettlauf um industrie- und technologiepolitische Führung: „Technologische Souveränität" im internationalen Vergleich'.

[331] Deutscher Bundestag (2024), 'Pläne der Bundesregierung zur Forschungssicherheit im Lichte der Zeitenwende'.

[332] Schwägerl (2024), 'Vom Weltgeist Zum Machthebel'; and Arcesati, Ghiretti, and Schwaag Serger (2023), 'In Research Collaboration, Drawing Red Lines with China Isn't Easy'.

[333] Devaux, and Schnitzler (2020), 'Defence Innovation: New Models and Procurement Implications. The French Case'.

[334] Ruitenberg (2024), 'France Preps Europe's Fastest Classified Supercomputer for Defense AI'.

[335] Devaux, and Schnitzler (2020), 'Defence Innovation: New Models and Procurement Implications. The French Case'.

[336] Niinistö (2024), *Safer Together – Strengthening Europe's civilian and military preparedness and readiness*.

[337] Angelier (2024), 'La Recherche Publique, Une Assurance Santé Pour Les Entreprises. Posologie: Abusez Des Cifre!'.

[338] Devaux, and Schnitzler (2020), 'Defence Innovation: New Models and Procurement Implications. The French Case'.

Finland: integrating total defence and innovation through a whole-of-society model

Finland's dual-use R&I strategy is shaped by its longstanding total defence doctrine – mobilising the entire society, including public agencies, private companies, and academia – to strengthen national resilience[339]. This whole-of-society approach supports the integration of civilian and defence innovation to address hybrid threats and critical technology vulnerabilities. Priority areas include cybersecurity, AI, secure communications, and critical infrastructure, with the government leveraging its telecom leadership – notably through Nokia – to develop secure 5G and 6G networks for both civilian and military use. NATO has recognised Finland's 6G research hub in Oulu as a key testbed for future defence communications[340], while Finnish efforts in quantum and AI are increasingly aligned with broader European security objectives[341].

Finland's innovation pipeline is built on structured collaboration between industry, academia, and defence agencies – a model codified in the country's national defence industry strategy[342]. The Finnish Defence Forces work closely with civilian institutions through initiatives such as the Centre of Excellence in Cyber Security, jointly developing solutions for national resilience and military-grade cybersecurity[343]. Business Finland supports dual-use innovation in domains like autonomous systems, Arctic infrastructure, and space-based surveillance through dedicated programmes and funding calls[344]. A distinctive feature of Finland's model is its expert reserve system, which enables the rapid mobilisation of civilian professionals – including engineers, cybersecurity experts, and logistics specialists – to support national security priorities[345].

Growing concerns over research security have led Finland to strengthen safeguards, aligning closely with EU and NATO standards. The Cyber Security Strategy (2024–2035) emphasises securing critical research infrastructure and tightening vetting of international collaborations, particularly in AI, quantum computing, and semiconductors[346]. The government has introduced stricter investment screening to prevent foreign acquisitions of sensitive technology firms[347], while Finland's deepening NATO integration enhances its capacity to protect critical innovations and contribute to European supply chain security[348].

Italy: strengthening dual-use R&I through EU collaboration and industrial integration

Italy has historically had a fragmented approach to dual-use R&I, with defence innovation tied primarily to procurement-driven modernisation rather than broader technology foresight[349]. However, recent strategic shifts – spurred by European Defence Fund (EDF) participation and increased engagement in NATO innovation frameworks – have begun to strengthen Italy's role in dual-use R&I. Italian actors have secured substantial EDF support in recent years, enabling collaborative projects in AI, quantum, and next-generation aerospace systems[350]. This growing involvement is gradually repositioning Italy within the European dual-use innovation landscape. Italy's recent defence planning documents and strategic initiatives – particularly those aligned with European defence cooperation and innovation – emphasize AI, cyber security, and aerospace, reflecting a growing commitment to long-term defence technology development[351]. Italy has also

[339] Järvinen (2024), 'Cautious Data-Driven Evolution: Defence AI in Finland'.
[340] O'Dwyer (2024), 'Finland to Host NATO Tech Centers, Revamp Cybersecurity Strategy'.
[341] Järvinen (2024), 'Cautious Data-Driven Evolution: Defence AI in Finland'.
[342] Ministry of Defence of Finland (2024), *Government Defence Report*.
[343] VTT, 'Cybersecurity Threat and Risk Management for Organisations'.
[344] Business Finland, 'Defense and Digital Resilience: New Global Competitive Edge from Comprehensive Digital Security and Defense'.
[345] National Defence Training Association of Finland, 'What Is the MPK?', available at: https://mpk.fi/en/.'
[346] Prime Minister's Office of Finland (2024), *Finland's Cyber Security Strategy 2024–2035*.
[347] Haanpää et al. (2025), 'Expansion of the Finnish FDI Screening Regime Expected'.
[348] Ministry of Defence of Finland (2024), *Government Defence Report*.
[349] Marrone, and Gilli (2020), 'Defence Innovation: New Models and Procurement Implications. The Italian Case'.
[350] CESAER (2024), 'Strengthen Dual-Use Technologies by Enhancing EU Defence Funding'; and Greenacre, and Matthews (2024), 'EU Commission Launches Bid to Expand Funding of Dual-Use Research in Horizon Europe's Successor'.
[351] Marrone, and Gilli (2020), 'Defence Innovation: New Models and Procurement Implications. The Italian Case'.

begun to increase its commitment to military R&D, reflecting a gradual shift away from dependence on imported systems and toward more strategic investment in domestic defence innovation[352].

Italy's dual-use innovation ecosystem is increasingly integrated into the European landscape. The country's defence industry, led by firms like Leonardo and Fincantieri, is leveraging EU partnerships to drive R&D, particularly in unmanned systems, advanced materials, and naval technologies[353]. Leonardo, for instance, coordinates multiple EDF projects including on next-gen helicopters, autonomous systems, and electronic warfare. Italy's regional tech clusters, such as those in Piedmont and Apulia, facilitate civil–military spillovers in robotics and aerospace[354]. The government also encourages spin-offs from defence research agencies, using initiatives like the Joint Center for Innovation (Centro Interforze per l'Innovazione), which connects defence researchers with industry and academia to commercialise military research into civilian applications. These efforts reflect a broader shift toward public–private collaboration to advance Italy's dual-use capabilities[355].

On research security, Italy has taken a more proactive stance by introducing national controls on dual-use exports, going beyond EU regulations to restrict emerging technology transfers to high-risk countries[356]. The country's Golden Power Law has been expanded to block foreign investment in strategic sectors such as AI, semiconductors, and biotech[357]. Additionally, Italian universities have begun to strengthen due diligence protocols, particularly in response to concerns over research collaborations in sensitive aerospace domains involving Chinese partners[358]. Italy's dual-use strategy reflects a hybrid model – balancing EU-supported innovation initiatives with national security measures to safeguard emerging technologies[359].

Poland: rapid expansion of dual-use R&I driven by security imperatives

Poland's dual-use R&I strategy has accelerated in response to regional security threats, particularly following Russia's war in Ukraine[360]. The government prioritizes autonomous systems, cyber defence, and secure communications, aligning its foresight efforts with NATO capability development. Government-backed efforts engage civilian AI and robotics firms to develop applications for defence and security, fostering civil–military tech transfer and building national resilience[361]. Poland also actively participates in NATO science programs and hosts joint R&D activities to embed Western technological expertise into its defence ecosystem[362].

The Polish innovation pipeline has benefited from offset agreements in defence procurement – securing technology transfers from major U.S. and European defence suppliers[363]. The Polish

---

[352] Marrone, and Gilli (2020), 'Defence Innovation: New Models and Procurement Implications. The Italian Case'.
[353] Leonardo, Collaborative Research Projects, available at: https://www.leonardo.com/en/innovation-technology/funded-research-projects.
[354] Italian Space Industry, 'Italian Aerospace Clusters'.
[355] Mundell (2022), 'The Ecosystem: In Europe, Defence Innovation Is the New Black'; Blagoeva et al. (2019), *Materials dependencies for dual-use technologies relevant to Europe's defence sector*.
[356] Marrone, and Gilli (2020), 'Defence Innovation: New Models and Procurement Implications. The Italian Case'; and Dell'Aquila et al. (2025), 'Towards An Ambitious FP10 – Shaping Europe's Role In The World Through Research And Innovation'.
[357] European Commission (2025), 'European Defence Fund: Over €1 Billion to Drive Next-Generation Defence Technologies and Innovation'.
[358] Arcesati, Ghiretti, and Schwaag Serger (2023), 'In Research Collaboration, Drawing Red Lines with China Isn't Easy'.
[359] CESAER (2023), 'Workshop on Research Security – GSF-01 Multilateral Dialogue on Principles and Values in International Research & Innovation Cooperation'; and Dell'Aquila et al. (2025), 'Towards An Ambitious FP10 – Shaping Europe's Role In The World Through Research And Innovation'.
[360] European Commission (2024), *White Paper on options for enhancing support for research and development involving technologies with dual-use potential*; and Kolliarakis (2022), 'Anticipatory Governance of Emerging and Disruptive Technologies with Dual-Use Potential'.
[361] Duszczyk (2025), 'Rodzimy sektor bezpieczeństwa potrzebuje polskich innowacji (The domestic security sector needs Polish innovations)'; and Chmielewski (2022), 'TECHNOLOGIE PRZEŁOMOWE W BUDOWIE ODPORNOŚCI PAŃSTWA'.
[362] Raubo (2024), 'Technologie podwójnego przeznaczenia wyzwaniem dla odporności kraju [OPINIA]'.
[363] Polski Fundusz Rozwoju, 'Rozwój technologii podwójnego zastosowania wspiera polską gospodarkę i bezpieczeństwo'.

Defence Fund, launched in 2022, provides venture capital to dual-use startups – mirroring similar efforts in Israel and the UK – and has become a key vehicle for accelerating military innovation[364]. Poland's research institutions are increasingly engaged in NATO's Science for Peace and Security Programme and EU-funded initiatives, including EDF and Horizon Europe, ensuring that domestic firms gain access to cutting-edge technologies[365]. These collaborations reflect Poland's growing commitment to strengthening defence R&D through both national and multilateral channels[366].

On research security, Poland enforces strict counterintelligence measures in academia, limiting collaborations with high-risk countries particularly Russia[367]. While there is no formal ban on academic collaboration, the Internal Security Agency (ABW) has been actively involved in uncovering foreign espionage networks operating in the country. Poland has also implemented cybersecurity regulations requiring research institutions and public entities to comply with national security standards, as outlined in its national cybersecurity strategy[368]. These measures reflect Poland's evolving role as a rapidly developing dual-use R&I hub, integrating international expertise while safeguarding its emerging technological base[369].

Sweden: leveraging high-tech industry and research excellence for dual-use innovation

Sweden's dual-use R&I strategy is primarily industry-driven – with companies like Saab and Ericsson leading in aerospace, secure communications, and sensor technologies[370]. While historically focused on civilian applications, Sweden has been gradually aligning with NATO and EU defence priorities – a trend that has significantly accelerated in the context of Sweden's NATO accession[371]. Emerging strengths in quantum, microelectronics, and photonics enhance capabilities in secure communications, AI-driven decision support, and electronic warfare. These are supported by initiatives such as the Wallenberg AI, Autonomous Systems and Software Program (WASP) and the Wallenberg Centre for Quantum Technology (WAQT)[372].

Sweden's dual-use innovation pipeline builds on a strong defence-industrial base, with companies such as Saab, Ericsson, GKN Aerospace, Bofors, and Hägglunds playing key roles in areas like defence systems, autonomous navigation, advanced sensing, and secure communications. The Esrange Space Center further strengthens national capabilities in space-based dual-use applications[373]. Sweden's civil–military pipeline is exemplified by initiatives such as the DAMM programme, which tests the VIKING uncrewed ground vehicle for autonomous defence applications[374]; and by Teledyne FLIR's and Axis Communications' Swedish-developed surveillance and imaging technologies serving both public and defence sectors[375]. Furthermore, the Civil-Military Innovation Programme, initiated by the Swedish Armed Forces and Vinnova, aims to enhance military capabilities through civil-military synergies[376]. Complementing this, the

[364] Kruczkowska (2024), 'Inwestycje dual-use: nowy trend czy rzeczywista potrzeba?'.
[365] European Commission (2025), 'European Defence Fund: Over €1 Billion to Drive Next-Generation Defence Technologies and Innovation'; and Blasi (2024), *Horizon Europe: Protecting academic freedom – Strengthening and improving implementation of Recital 72*.
[366] Raubo (2024), 'Technologie podwójnego przeznaczenia wyzwaniem dla odporności kraju [OPINIA]'; and Ministerstwo Obrony Narodowej (2024), 'Resortowa strategia sztucznej inteligencji do roku 2039'.
[367] Reuters (2024), 'Poland Investigating Russian Espionage, Security Agency Says'.
[368] Ministerstwo Obrony Narodowej (2024), 'Resortowa strategia sztucznej inteligencji do roku 2039'.
[369] Polski Fundusz Rozwoju, 'Rozwój technologii podwójnego zastosowania wspiera polską gospodarkę i bezpieczeństwo'.
[370] Teknikföretagen, and SOFF (2023), 'En nationell teknologi- och innovationsstrategi som främjar dual use'; and Government Offices of Sweden (2024), *Strategic Direction for Defence Innovation*.
[371] Marklund et al. (2023), *Omvärldsanalys - Analysbilaga till Vinnovas Underlag till Regeringens Forsknings- Och Innovationspolitik*.
[372] Strander et al. (2023), 'Acceleration mot en hållbar framtid - Vinnovas inspel till regeringens forsknings- och innovationsproposition'.
[373] Teknikföretagen, and SOFF (2023), 'En nationell teknologi- och innovationsstrategi som främjar dual use'.
[374] Defence Industry Europe (2025), 'Sweden Procures VIKING Uncrewed Ground Vehicle for Autonomous Military Programme'.
[375] FLIR (2022), 'Teledyne FLIR Helps to Keep Airspace Surrounding Swedish Critical Infrastructure Free of Drones'; Axis Communications, available at: https://www.axis.com/sv-se.
[376] Government Offices of Sweden (2024), *Strategic Direction for Defence Innovation*.

Swedish Government's research and innovation proposition includes substantial investments in groundbreaking technologies to bolster Sweden's capabilities in dual use R&I[377].

In response to evolving geopolitical dynamics, Sweden has intensified its focus on research security by promoting responsible internationalisation across higher education, research, and innovation. As part of a government assignment, the Swedish Council for Higher Education (UHR), the Swedish Research Council, and Vinnova jointly developed national guidelines and proposed the establishment of a national support function aimed at strengthening the capacity of entire research and innovation ecosystems – including universities, incubators, and startups in sensitive areas such as dual-use technologies – to manage international collaborations securely[378]. The overarching goal is to safeguard national interests while maintaining Sweden's traditionally open research environment[379]. In parallel, the Swedish Security Service (Säpo) has issued public warnings about foreign espionage targeting strategic technologies, prompting actors in the dual use R&I ecosystem to introduce stricter screening and compliance procedures[380]. These developments reflect Sweden's shift toward a more structured and security-conscious approach to international research cooperation.

United Kingdom: leveraging defence-led foresight and strategic partnerships in dual-use R&I

The United Kingdom has established itself as a key European player in dual-use R&I, aligning its technology priorities with national security and economic resilience. The Integrated Review Refresh (2023) identifies AI, semiconductors, quantum technologies, and synthetic biology as critical areas, integrating foresight efforts across civilian and defence applications[381]. Strategic funding mechanisms, including the National Security Strategic Investment Fund (NSSIF) and Innovate UK, provide early-stage support for dual-use technology development[382]. Public-private partnerships play a crucial role, with the UK leveraging its defence-industrial base and specialized innovation hubs to accelerate civil-military technology transfer[383].

The UK's innovation pipeline is supported by initiatives such as the Defence and Security Accelerator (DASA), which identifies and funds emerging technologies with military applications, including autonomous systems, cyber defence, and secure communications[384]. Procurement reforms facilitate SME participation in defence contracts, ensuring a diverse and competitive innovation landscape[385]. The UK's close collaboration with key allies, particularly through AUKUS and bilateral partnerships with Israel and Japan, enhances its access to cutting-edge R&D[386]. Participation in NATO's Defense Innovation Accelerator (DIANA) and the NATO Innovation Fund further integrates the UK into international dual-use research ecosystems[387].

Research security measures have been strengthened to protect national interests while maintaining an open research environment. The National Security and Investment Act (2021) restricts foreign influence in critical technology sectors[388], while the Academic Technology Approval Scheme (ATAS) regulates access to postgraduate STEM fields for foreign students[389].

---

[377] Regeringskansliet (2024), 'Excellent forskning och innovationskraft premieras i den största forsknings- och innovationspropositionen någonsin'.
[378] Swedish Council for Higher Education, Swedish Research Council, and Vinnova (2024), *National Support Function for Responsible Internationalisation – Final Report 2025*.
[379] Arcesati, Ghiretti, and Schwaag Serger (2023), 'In Research Collaboration, Drawing Red Lines with China Isn't Easy'.
[380] Säkerhetspolisen (2024), *Säkerhetspolisen 2024-2025*.
[381] UK Government (2023), *The UK's International Technology Strategy*.
[382] British Business Bank, 'National Security Strategic Investment Fund'; and British Business Bank, 'About NSSIF'.
[383] KARVE (2023), 'UK Defence Innovation Funds & Accelerator Programmes'.
[384] Defence and Security Accelerator (2024), 'Defence and Security Accelerator - Strategy 2024-26'.
[385] TechUK (2025), 'Ministry of Defence Announces New Support for SMEs'.
[386] Silverberg, Sharpe, and Murray (2025), 'Making AUKUS work: The case for an Indo-Pacific defense innovation consortium'.
[387] UK Government (2024), 'NATO DIANA UK accelerator: Welcome to the UK accelerator'.
[388] UK Government (2024), 'National Security and Investment Act: guidance for the higher education and research-intensive sectors'.
[389] UK Government (2013), 'Academic Technology Approval Scheme (ATAS)'.

The Trusted Research Guidelines and the Research Collaboration Advice Team (RCAT) provide academia and industry with risk management tools for international partnerships[390]. By balancing security concerns with scientific openness, the UK sustains its role as a global leader in dual-use innovation, ensuring resilience against emerging geopolitical and technological challenges[391].

3.4. Observations

Drawing on the international comparison of dual-use R&I strategies, a number of cross-cutting observations emerge that reflect how countries are responding to shared challenges in this domain. The EU context is shaped by a dual imperative: to make better use of its scientific and industrial strengths, including for security purposes, while safeguarding core values such as openness, transparency, and democratic accountability. The observations below highlight common patterns and emerging practices in national and international strategies, with relevance for actors seeing to better understand the conditions that shape effective dual-use innovation ecosystems.

Shared responsibility is a key enabler of dual-use R&I: Across advanced dual-use ecosystems – notably in the United States and Israel – trust-based collaboration between government, research institutions, investors, and defence actors play a central role in enabling both security awareness and opportunity-driven innovation. These ecosystems are marked by a shared understanding of roles and responsibilities and long-term strategic alignment. The evolution of the Silicon Valley, supported by enduring public–private partnerships, and Israel's integrated civilian–military R&I environment illustrate how institutionalised collaboration can underpin adaptive and resilient innovation systems. In several contexts, shared responsibility is closely linked to coordination across sectors and a mutual awareness of the dual-use implications of emerging technologies.

Trusted networks are shaping the future landscape of international collaboration: In response to shifting geopolitical conditions, countries such as Finland, France, and others are engaging in structured bilateral and minilateral partnerships to advance dual-use technologies alongside trusted international actors. Examples include initiatives such as NATO DIANA and other forms of security-oriented R&I cooperation. These arrangements reflect a broader trend toward selectively deepening cross-border collaboration on dual-use innovation in ways that support shared technological, security, and industrial priorities.

Strategic foresight and innovation pipelines are increasingly integrated: Many governments are combining foresight mechanisms – such as technology roadmaps and horizon scanning – with innovation support instruments, including accelerators and venture funding schemes. This approach can be seen in INNOFENSE (Israel), DASA (United Kingdom), and the Defense Innovation Unit (United States), which connect early-stage innovation to capability needs through structured funding and scouting. In Finland, dual-use priorities are embedded in both national innovation and security strategies. At the EU level, Horizon Europe and the European Defence Fund remain institutionally separate, although coordination efforts are increasing. Several international cases illustrate how foresight functions are used to guide investment priorities and shape innovation pipelines. Alongside these spin-in models, structured mechanisms for spinning off defence-funded research into civilian markets – such as NASA's technology licensing programme or the UK's Ploughshare Innovations – also play a significant role in maximising the public value of dual-use investments, whether through formal channels or ecosystem-driven innovation pathways such as the Silicon Valley case.

Balancing openness with security is a growing governance priority: Countries are developing regulatory and procedural frameworks to address risks linked to foreign interference, knowledge leakage, and sensitive technology transfer. Finland and Sweden are examples of Member States introducing national due diligence guidelines, while Germany has strengthened institutional

[390] National Protective Security Authority (2024), 'Trusted Research Guidance for Senior Leaders'.
[391] British Council, and Universities UK International (2024), 'Managing Risk and Developing Responsible Transnational Education (TNE) Partnerships'.

support for research security and IP management. Ethics and security screening are part of Horizon Europe's project evaluation processes, and recent discussions on research security suggest a growing awareness of risk-related considerations in funding governance. At the EU level, the Council Recommendation on Research Security (2024) and the Economic Security Strategy provide Member States with a common framework for due diligence and knowledge protection. These developments point to a broader convergence in how countries approach the governance of dual-use research, reflecting concerns about strategic autonomy and responsible international engagement.

Talent and workforce development are gaining strategic importance: A growing number of countries are investing in capacity-building for dual-use innovation, particularly in domains such as AI, cybersecurity, and advanced materials. France and Germany, among others, have introduced mobility schemes, training programmes, and dual-use ethics content targeting researchers and entrepreneurs. Startup visa programmes and tailored support for early-stage companies also reflect increased attention to talent attraction and retention. Across several countries, workforce development is becoming more explicitly linked to national security objectives and to the long-term viability of dual-use R&I ecosystems.

4. Funding programmes for dual-use research and innovation – an international comparison

4.1. Introduction

This chapter studies dual-use R&I funding systems and programmes from two complementary perspectives. The first section explores dual-use programmes in several countries around the world and NATO, identifying their salient features, connections with R&I programmes of a purely civilian or defence nature, and broader national or organisational context. This outline provides international benchmarks and helps to identify different approaches to dual-use R&I.

The second section then takes a comparative perspective, finding both commonalities in the surveyed funding programmes as well as differences between them. Together with the overview presented in the first section, it provides a better understanding of the relative merits of the programmes described here, guiding the design of new programmes.

In the final part of this chapter, a small selection of lessons learnt is distilled and a blueprint for the design and implementation of new dual-use funding programmes is outlined.

The data used for this chapter originates from three main sources. First, evidence was gathered with the help of European Commission's diplomatic staff posted in relevant EU delegations, covering several of the funding systems that will be described in this chapter. This input draws upon a number of sources, all of which are publicly available. Second, contact was made with colleagues, diplomats, or officials from the United States, Japan, the United Kingdom, Finland, and NATO. Third, information was obtained directly from legislation and similar public sources to provide a more comprehensive picture. The foregoing notwithstanding, the topic of dual-use technologies, even in the context of R&I, is a sensitive one in many parts of the world. The information collected therefore varies in volume and detail. To present a thorough picture, however, as much information as possible has been presented, even if some details are only available for few of the systems surveyed.

There is a significant heterogeneity between the funding systems surveyed in this chapter. Hence, a number of topics are identified which allow the construction of a coherent narrative that, on the one hand, helps to expose commonalities and differences amongst the various systems and, on the other, highlights factors that should be considered in the development of dual-use funding systems in a region as varied as the EU. The first aspect considered is the *rationale* underlying the existence of each surveyed dual-use funding system, e.g., geopolitical, economic, or otherwise. The second is *policy*, i.e., how the system is governed; whereas evidence of success can be seen in several contexts, the distinction between, e.g., top-down challenge-driven versus bottom-up curiosity-driven systems is a very pertinent one in the European context. Third, the *internationalisation* aspects of the programmes varied greatly, providing much material that could help support decisions to be taken at the EU level, where defence is largely seen as a competence of individual Member States. Fourth, *fragmentation* of the studied funding systems was not just a factor that affected the quality of this chapter itself – a highly fragmented system easily becomes a very opaque one –, but it allows to consider the trade-off between many ways of targeting various parts of the dual-use ecosystem. Fifth, *bridge-building* between civilian and defence markets is an important feature of many dual-use research systems that, one could argue, is an important contribution to their success.

It is important to acknowledge at the outset that this chapter is limited in scope: (i) The selection of countries and organisations is not exhaustive; (ii) the quality of data available varies greatly between the studied funding systems; (iii) due to the differences in philosophies and nature of the dual-use funding systems studied, it was often the case that programmes or features did not map naturally across systems; (iv) the distinction between dual use and other kinds of research is not always made explicit, such that obtaining figures for the funding made available to dual-use

research is sometimes impossible; and (v) some key dual-use and defence funding systems are set up to exclusively cater for a national audience, requiring the use of machine translation for extracting details from primary sources.

4.2. Funding dual-use R&I around the world

4.2.1. North America

United States of America[392]

Box 9: DARPA: The gold standard in developing world-changing technologies

DARPA (Defense Advanced Research Program Agency) is considered one of the most successful models for government-funded dual-use research. It prioritises use-inspired research, both in answer to specific challenges and in the spirit of creating new technologies. Two key aspects of DARPA are its light management and the steering of its research by program managers who are technical experts; these are credited as helping to create a uniquely successful funding programme. The global positioning system (GPS) and the Internet are two world-changing technologies that were, in part at least, spearheaded by DARPA.

Source: The author

Policy background

Policymaking related to dual-use technologies (including research and innovation aspects) falls under the remit of several departments of the US government:

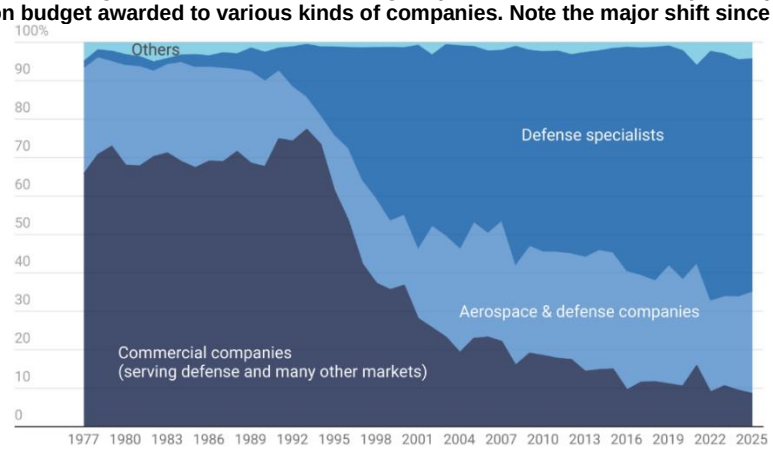
- The US Department of Defense (DOD) launched the Defense Innovation Initiative in 2014 to help advance US national security interests. The Long-Range Research and Development Project Plan (LRRDPP) is part of this effort and is intended to help provide the US with military technology advantage through new and emerging technologies. LRRDPP has five main focus areas: air, missile, and precision-guided munition defence; air superiority; space; undersea; and emerging technologies. In its mission "attract ideas from across the defence industrial base, commercial industry, government and individuals,"[393] the LRRDPP also promotes dual-use technologies. Broader policy defence and dual-use priorities in the US follow a multi-layered approach. At the highest level there is the National Defense Strategy compiled by the DOD, which sets the strategic direction of the DOD to support US national security priorities and includes passing references to threats stemming from dual-use technologies,[394] particularly in the nuclear sector. Within the DOD itself, the Defense Innovation Board[395] is an advisory committee that issues independent recommendations to the Secretary of Defense and the senior leadership of the DOD on, amongst other matters, emerging technologies.
- The US Department of Energy (DOE) operates the Office of Critical and Emerging Technologies[396], which has access to the expertise both within the DOE itself and the National Laboratories operated by the DOE. It plays multiple roles, including supporting and informing policymaking as well as developing partnerships to integrate emerging technologies into the commercial market.

[392] The original financial numbers in this section were expressed in USD; an approximate conversion is being made to EUR for the purposes of comparison across countries.
[393] U.S. Department of Defense Innovation Marketplace, 'Long-Range Research and Development Program Plan'.
[394] U.S. Department of Defense (2022), *2022 National Defense Strategy of the United States of America*.
[395] U.S. Department of Defense, Defense Innovation Board, available at: https://innovation.defense.gov/About1/.
[396] U.S. Department of Energy, 'Office of Critical and Emerging Technologies', available at: https://www.energy.gov/cet/office-critical-and-emerging-technologies.

- The US Department of State (DOS) hosts the Office of the Special Envoy for Critical and Emerging Technology[397], whose role is both to coordinate the DOS's internal work on critical and emerging technologies, such as artificial intelligence, biotechnology, and quantum information science, and to act as a focal point to make critical and emerging technologies a central feature of US diplomacy.

Aside from these aspects, it is important to note that the US defence market underwent a major shift in recent decades. Prior to the end of the 1980s, the main commercial operators working in the US defence sector were commercial companies with broader interests than defence. Since the 1990s (see Figure 12), defence specialists, which have no commercial interests other than defence, have become the dominant aspect of the US defence market. Despite this shift, and the focus on dual-use technologies, issues persist hindering startups and SMEs from working with the DOD including the plethora of rules, regulations, and policies governing dual-use technologies. Amongst the regulations that apply to dual-use technologies and the broader defence market in the US are the Defense Federal Acquisition Regulation Supplement (DFARS) and the Federal Acquisition Regulation (FAR), with DFARS supplementing FAR. Companies aiming to supply civilian goods and services to the US government typically have to comply with FAR, which includes carve-outs for smaller awards (less than about EUR 2 million). Defence acquisitions, however, are subject to the more onerous DFARS, which presents an unwieldy burden for small businesses.

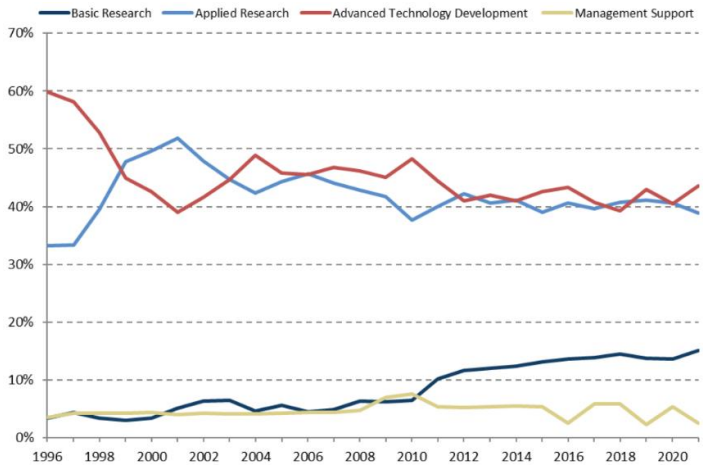
Figure 12: The evolving US defence market. This figure plots the share of the major weapons systems acquisition budget awarded to various kinds of companies. Note the major shift since the 1990s.



Source: Center for Strategic and International Studies, *Why Is the U.S. Defense Industrial Base So Isolated from the U.S. Economy?* (2024).

[397] U.S. Department of State, 'Office of the Special Envoy for Critical and Emerging Technology', available at: https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-special-envoy-for-critical-and-emerging-technology/.

Figure 13: Share of DARPA funding by character of work, 1996–2021.



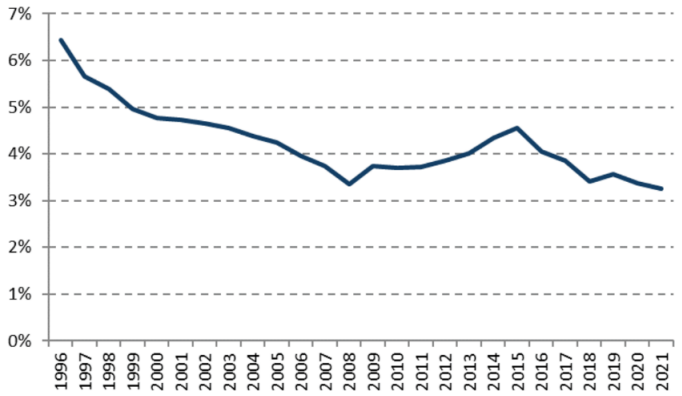
Source: US Congressional Research Service, *Defense Advanced Research Projects Agency: Overview and Issues for Congress* (2021).

Funding of dual-use R&I

Funding for projects in the US dual-use R&I system is dominated by the Department of Defense through a number of initiatives and agencies:

- The DOD's Defense Advanced Research Projects Agency (DARPA) is often cited as the standard model to emulate[398] when seeking to fund research projects in defence or dual-use technologies. Critically, and unlike other agencies in the US, DARPA aims to fund innovations that not only solve current challenges but help the US lead in strategic technological invention. DARPA had an annual budget of approximately EUR 3.8 billion in 2024[399] (slightly less than the original request, which remained essentially unchanged for 2025[400]) and is divided into several offices, covering biological technologies, defence sciences, information innovation, microsystems technology, strategic technology, and tactical technology.

Figure 14: DARPA funding as a share of the funding allocated to the US Department of Defense Research, Development, Test, and Evaluation Programmes, 1996–2021.

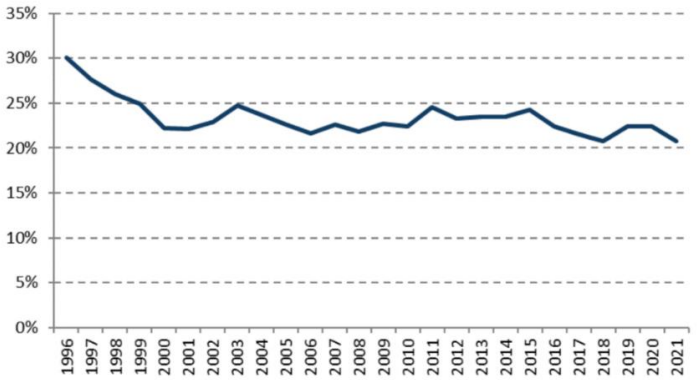


Source: US Congressional Research Service, *Defense Advanced Research Projects Agency: Overview and Issues for Congress* (2021).

[398] Dugan and Gabriel (2013), '"Special Forces" Innovation: How DARPA Attacks Problems'.
[399] Defense Advanced Research Projects Agency, 'Budgets and Testimony'.
[400] U.S. Department of Defense (2024), 'Fiscal Year (FY) 2025 Budget Estimates'.

In recent years, DARPA has been allocating approximately 40% of its budget to each of applied research and advanced technological development, with an additional approximately 15% being reserved for basic research programmes (Figure 13). Interestingly, DARPA has been allocated a declining share of the funding allocated to the US Department of Defense Research, Development, Test, and Evaluation Programmes (Figure 14), declining from approximately 6% in 1996 to about 3% in 2021[401].

Figure 15: DARPA funding as a share of defence science and technology funding, 1996–2021.



Source: US Congressional Research Service, *Defense Advanced Research Projects Agency: Overview and Issues for Congress* (2021).

Nevertheless, the funding allocated to DARPA as a share of defence science and technology funding allocated by the US has remained stable at between 20% and 25% since before 2000[402] (Figure 15). Combining available data from 2019[403] and 2025[404] shows that the US allocates approximately 1.7% of the federal R&D budget, or approximately 0.02% of its GDP[405], to DARPA.

The outsized success of DARPA makes it a reference point for government R&D programmes. In this respect, three of its key differentiators are[398]: a reliance on ambitious goals intended to solve real-world problems or create new opportunities rather than open-ended research programmes; organisation through fixed-term expert technical managers; and independence in selecting and running projects, which allows it to take risks. In entering into agreements with for-profit contractors, DARPA is furthermore empowered to enter into Other Transactions (OTs), which are exempt from the Bayh–Dole Act, which grants the US government a non-exclusive royalty-free license for inventions resulting from the contract.[406] OTs thus give contractors substantially greater flexibility in negotiating intellectual property rights with DARPA.[407]

- The DOD has historically allowed firms receiving funds to use some of their general and administrative expenses to cover independently research and development, so long as these efforts are of potential interest to the DOD. This Independent Research & Development (IR&D) initiative is complemented by the DOD's Defense Innovation Marketplace (DIM), which acts as a communications channel between the DOD and companies implementing IR&D projects. The DIM also includes a Defense Innovation Unit (DIU), which is focused exclusively on scaling commercial technology across the US military at commercial speeds by engaging directly within

[401] Congressional Research Service (2021), 'Defense Advanced Research Projects Agency: Overview and Issues for Congress'.
[402] *Ibidem*.
[403] Congressional Research Service (2018), 'Defense Advanced Research Projects Agency: Overview and Issues for Congress'.
[404] Congressional Research Service (2024), 'Federal Research and Development (R&D) Funding: FY2025'.
[405] World Bank, 'GDP (current LCU) - United States'.
[406] Defense Advanced Research Projects Agency (2024), 'Protecting Innovation: Understanding IP in DARPA Contracts'.
[407] Defense Advanced Research Projects Agency (2012), 'Doing Business With DARPA: Creating and Preventing Strategic Surprise'.

the venture capital and commercial technology innovation ecosystem across seven critical technology sectors (artificial intelligence, autonomy, cyber and telecom, emerging technology, energy, human systems, and space); the average time to issue an award for a protype stood at 197 business days in 2023408. In 2024, the DIU had a strategic budget of about EUR 900 million.

- The US government also operates a number of National Laboratories, including Lawrence Livermore National Laboratory (LLNL), which applies science and technology to defence and is part of the DIM. LLNL has several mission areas, including nuclear deterrence, stockpile and enterprise transformation, threat preparedness and response, biological resilience, climate and energy security, climate resilience, multi-domain deterrence, and strategic advantage. In 2024 it had a budget of approximately EUR 3 billion[409], funded through a number of sources.

The US also operates many funding agencies, some of whom are of relevance to research in dual-use technologies:

- Following the DARPA model to an extent, the US government also operates the Advanced Research Projects Agency for Health (ARPA-H), with a budget of approximately EUR 1.4 billion allocated in 2024[410], and the Advanced Research Projects Agency for Energy (ARPA-E), with a budget of approximately EUR 450 million in 2023[411].
- The National Science Foundation (NSF) Directorate for Technology, Innovation and Partnerships, which positions itself between the basic research focus of the rest of the NSF and the far more applied focus of DARPA.

The US has a large and complex system for allocating federal funding to dual-use R&D. Although the flagship DARPA is allocated an annual budget of approximately EUR 4 billion, in 2025 the Department of Defense was allocated an R&D budget of approximately EUR 85 billion[412] (0.33% of GDP). Meanwhile, the 2025 US federal R&D allocation in the aggregate was of approximately EUR 185 billion[413] (0.73% of GDP). Within these figures, however, it is difficult to estimate specific budgets allocated to dual-use R&I, since no evidence of ring-fencing was found.

Beyond the government funding ecosystem, the US has a highly evolved private venture capital market. Amongst the firms that regularly invest in defence or dual-use technologies are Sequoia Capital, and Andreessen Horowitz, aside from many smaller firms. More than EUR 110 billion in venture capital funding was invested in US defence technology startups between 2021 and 2023[414].

The complementarity of public and private funding in the US is exemplified by the DIU of the DOD. It is estimated that the total of ca. EUR 5.1 billion of contracts awarded by the DIU between 2016 and 2023 leveraged a further ca. EUR 63 billion of private investment[415].

International dimension

US research programmes involving dual-use technologies maintain strict controls on international participation. Programmes may require US citizenship or permanent residency, since sharing any dual-use information with someone who is neither a US citizen nor a US permanent resident could be considered a “deemed export” and subject to export control[416]. This barrier to international cooperation has been recognised as being counter-productive, with a recent report by the Defense Innovation Board[417] making a case for stronger linkage between the US and its allies in developing

[408] U.S. Department of Defense (2024), *The Defense Innovation Unit FY 2023 Annual Report*.
[409] Lawrence Livermore National Laboratory, ‘By the Numbers’.
[410] Advanced Research Projects Agency for Health, ‘Budget and Appropriations’.
[411] Advanced Research Projects Agency for Energy (2024), ‘FY 2024 Congressional Justification’.
[412] Congressional Research Service (2024), *Federal Research and Development (R&D) Funding: FY2025.*
[413] *Ibidem.*
[414] Sagamore Institute (2024), ‘Defense Tech Investments’.
[415] U.S. Department of Defense (2024), *The Defense Innovation Unit FY 2023 Annual Report.*
[416] University of Wisconsin – Green Bay, ‘Export Controls’, Office of Grants & Research.
[417] Defense Innovation Board (2024), *Optimizing Innovation Cooperation with Allies and Partners*.

innovative technologies. Although data for international activities is sparse, the DIU reports issuing a total of about EUR 70 million in awards to international partners between 2016 and 2022, approximately 6% of the total contract value it awarded over the same period[418].

Export of dual-use technologies is subject to several pieces of legislation, resulting in a rigid and complex export control system. The Department of State, through its Directorate of Defense Trade Controls, is responsible for the export and temporary import of defence articles and services as governed by the Arms Export Control Act, as implemented by the International Traffic in Arms Regulations[419] (ITAR), and Executive Order 13637[420]. Of concern to commercial entities is that ITAR may impose two further burdens:

- The extraterritoriality rule means that certain items or technologies that were originally exported from the US to a second country are subject to an export control license from the US even if they are being sold on to a third country.
- The see-through rule means that a product which includes a component controlled under ITAR would itself fall under ITAR control; an ITAR chip in a plane, for example, puts the entire plane under ITAR control.

Export of dual-use technologies more broadly are governed by the Export Administration Regulations[421] (EAR), managed by the Bureau of Industry and Security. Export control licensing under the EAR is generally easier than under the ITAR regime.

One final aspect of the international dimension of dual-use R&I in the US is that of business transactions. The Committee on Foreign Investment in the United States[422], within the Department of the Treasury, is authorised to review certain transactions involving foreign investment in the US as well as certain real estate transactions by foreign persons, with the aim of determining the effect of these transactions on US national security.

4.2.2. Asia-Pacific

People's Republic of China

Box 10: Becoming a leader through top-down action: Quantum communications

Quantum communications, which allows for the building of ultra-secure communication systems, was first mentioned by the Chinese leadership as part of its 13th Five-Year Plan in 2015, three decades after the birth of the field in North America and many years following initial steps towards its commercialisation in Europe. Through a top-down focus, China managed to establish itself as the leader of the field and presently boasts both the largest quantum network anywhere in the world, including two quantum communication satellites, and is the global leader in domestic quantum communication patents.

Source: The author

Policy background

The People's Republic of China's[423] (PRC's) approach to dual-use R&I cannot be viewed separately from its broader R&I ecosystem and the overall scientific and military ambitions of its leadership; in other words, the PRC leadership does not formally distinguish between research that is civilian in nature and that which serves military purposes. Research, innovation, and the development of technologies, including dual-use, are largely set in a top-down fashion by the government, through long-term strategies – such as the Five-Year Plans announced periodically by the leadership of the PRC – and consequent long-term investments.

[418] U.S. Department of Defense (2024), *The Defense Innovation Unit FY 2023 Annual Report.*
[419] Cornell Law School (2023), 'International Traffic in Arms Regulations (ITAR)', Legal Information Institute.
[420] U.S. Federal Government (2013), Executive Order 13637—Administration of Reformed Export Controls.
[421] U.S. Bureau of Industry and Security, 'About Export Administration Regulations (EAR)'.
[422] U.S. Department of the Treasury, 'CFIUS Overview'.
[423] This report sometimes uses "China" as a short-hand way of referring to the People's Republic of China (PRC).

Until recently[424], the thrust of the PRC's programme to develop dual-use technologies followed a model known as Civil–Military Integration (CMI), which has now evolved to a more comprehensive one termed Military–Civil Fusion (MCF). In the 14th Five-Year Plan for Economic and Social Development (2021-2025) and the Long-Ranged Objectives for 2025[425], one notes intentions, for example, to "promote resource sharing of military and civilian research facilities; and facilitate the two-way application of military and civilian scientific research achievements"[426]. Although the shift between CMI and MCF may seem subtle, it exemplifies a shift in the strategic thinking of the PRC. Whereas the former strategy aimed to combine military and civilian sectors, the present one fundamentally blurs the lines between civilian and military sectors, thus serving both security and economic objectives simultaneously. Under the MCF there is also emphasis on the PRC acquiring intellectual property and key research to advance its military aims.

Funding of dual-use R&I

The Ministry of Science and Technology of the PRC launched a comprehensive national R&D programme in 1986[427] that included provisions for advancing space and satellite technologies many aspects of which are of an inherently dual-use nature[428]. This programme was terminated in 2016 and replaced by the National Key Research and Development Plan. In 1986 the PRC also created the National Natural Science Foundation of China (NSFC)[429], which presently supports fundamental research across a broad spectrum of technological fields, including those with dual-use potential such as artificial intelligence, aerospace, and quantum technologies. Applications to defence or national security are mentioned in the NSFC's Guide to Programmes[430]. The Made in China 2025 strategy[431], launched in 2015, targets several key sectors for government support to boost the PRC manufacturing industry, and explicitly mentions both national security and defence applications. There is no evidence that specific budgets are ring-fenced for funding of dual-use R&I since the PRC does not distinguish between civilian or military research in any way. In 2019, the declared R&D budget of the PRC was ca. EUR 390 billion[432] (2.4% of GDP[433]), which compares favourably with the overall military expenditure (ca. EUR 270 billion[434] and 1.7%, respectively).

International dimension

The PRC encourages international collaboration in some areas, particularly in basic science[435], although laws surrounding data protection and security have increased scrutiny on foreign researchers in recent years with the aim of preventing the leakage of sensitive data outside the PRC.[436] Furthermore, dual-use and defence-related technologies are subject to strict controls intended to prevent technology leakage, particularly for sensitive technologies with military applications. The PRC's robust export control regime is managed by the Ministry of Commerce (MOFCOM), and focuses on technologies with military applications. In December 2024, the Regulations on Export Control of Dual-Use Items and Export Control List of Dual-Use Items took effect[437]. These regulations aim at control not just the transfer of dual-use items outside Mainland China, but also to foreign entities and individuals. They also establish a uniform list of dual-use

[424] Fritz (2019), 'China's Evolving Conception of Civil-Military Collaboration'.
[425] The People's Republic of China State Council (2021), 'Outline of the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Long-Range Objectives Through the Year 2035'.
[426] The People's Government of Fujian Province (2021), 'Outline of the 14th Five-Year Plan (2021-2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China'.
[427] Ministry of Science and Technology of the People's Republic of China, 'National High-tech R&D Program (863 Program)'.
[428] Nouwens and Legarda (2018), 'China's pursuit of advanced dual-use technologies'.
[429] National Natural Science Foundation of China, available at: https://www.nsfc.gov.cn/english/site_1/index.html.
[430] National Natural Science Foundation of China (2023), *National Natural Science Fund Guide to Programs 2023.*
[431] Center for Security and Emerging Technology (2022), 'Translation of PRC State Council (2015) *Notice of the State Council on the Publication of "Made in China 2025"*'.
[432] World Bank, 'Research and development expenditure (% of GDP) – China'.
[433] World Bank, 'GDP (current LCU) – China'.
[434] World Bank, 'Military expenditure (% of GDP) – China'.
[435] National Natural Science Foundation of China, available at: https://www.nsfc.gov.cn/english/site_1/index.html.
[436] Matthews (2025), 'Foreign researchers in China face tightening restrictions'.
[437] Zhu et al. (2024), 'China's New Export Control Framework: Key Changes for Dual-Use Items'.

items, facilitate dual-use exports, establish an export watch list, and extend the extraterritorial reach of MOFCOM in the case of dual-use items.

Japan[438]

Box 11: Horizon scanning: Consulting with dual-use startups in Japan

The explicit support of dual-use R&I is a relatively new concept in Japan, which has a strict constitutionally mandated pacifist stance. To help catalyse the development of a dual-use ecosystem and to maximise the potential for economic development, the Japanese Ministry Economy, Trade and Industry was tasked with curating a list of, and meeting with, startups that could have technologies with dual-use potential. This helps the government to get a good sense of what technologies exist in the local ecosystem that could be nurtured and grown for the benefit of both national security and economic growth.

Source: The author.

Policy background

Defence in general, and dual-use research in particular, are seen as controversial topics in Japan. Academics[439] have repeatedly voiced opposition to moves perceived as encouraging the use of scientific research for non-civilian purposes. Nevertheless, attitudes seem to be changing across society. The Science Council of Japan (SCJ) has been discussing the issue of dual-use technologies (particularly in the context of nuclear power[440]) since the 1960s and has recently adopted a softer stance towards dual-use research. Whereas in 2017 the SJC was responsible for a boycott of a research programme that targeted dual-use research[441], by 2022 its official opinion was that the separation between civilian and military technologies is not straightforward[442]. This break with the past contributed to an increased acceptance of dual-use research by the Japanese academic community. It occurred shortly following the increased involvement of Japanese government ministries in dual-use research, which can be traced to the launch of research and development funding in the area of defence and dual-use by the Japanese Ministry of Defence in 2015[443].

Funding of dual-use R&I

Three entities within the Japanese government are actively involved in funding dual-use research: the Ministry of Economy, Trade and Industry, the Ministry of Defence, and the Cabinet Office.

- The Ministry of Economy, Trade and Industry (METI) produced a position paper in 2024[444] on how to set up a dual-use startup ecosystem in Japan[445]. METI is responsible to meet with and curate a list of startups that may be in possession of dual-use technologies[446] and who will proactively be invited to pitch solutions to government policy issues. In addition, existing startup support programmes will be made available for dual-use technologies, including NEDO Deep Tech Startup Support[447], which takes the form of R&D support for the seed or early development phases and is dependent on venture capital support (2023 budget ca. EUR 600 million with a limit of ca. EUR 18 million per project); Go-Tech projects, which support R&D within SMEs, universities, and research institutes (annual budget ca. EUR 87 million with a limit

[438] The original financial numbers in this section were expressed in JPY; an approximate conversion is being made to EUR for the purposes of comparison across countries.
[439] Japanese Coalition Against Military Research in Academia, available at: http://no-military-research.jp/.
[440] Japan Society for the Promotion of Science (2015), *For the Sound Development of Science: The Attitude of a Conscientious Scientist*.
[441] Cyranoski (2017), 'Japanese scientists call for boycott of military research'.
[442] Ikeda (2022), 'Japan science council says drawing line between military, civil use technology difficult'.
[443] Japan Ministry of Defence, 'Research & Development'.
[444] Japan Ministry of Economy, Trade and Industry (2024), 'Towards building a dual-use startup ecosystem'.
[445] Gehrke (2024), 'METI's "Towards building an ecosystem for dual-use startups" report'.
[446] Prosser (2023), 'Japan aims to boost defense industry with 200 startups'.
[447] New Energy and Industrial Technology Development Organization (2024), 'Deep-Tech Startups Support Program (DTSU), Deep-Tech Startups Support Program in the Green Transformation field (GX)'.

of ca. EUR 600,000 annually per project); and J-Star projects, which support sending young entrepreneurs abroad (annual budget ca. EUR 40 million).

- The Ministry of Defence operates not only on the principle of identifying the needs of the country and subsequently looking for solutions that may satisfy those needs, but it actively probes the private sector to understand the nature and promise of cutting-edge technologies and how they may be deployed in the defence ecosystem. To assist it in performing this mission, in October 2024, the Ministry launched the Defense Innovation Science and Technology Institute (DISTI)[448], under the Acquisition, Technology and Logistics Agency, reportedly to be modelled after DARPA[449], '*to explore the various possibilities of science and technology, make breakthroughs that defy conventional knowledge'* and speed up the uptake of science and technology to lead to innovation in defence[450]. In its 2024 budget, the government of Japan was reported[449] to have set aside approximately EUR 134 million to fund DISTI. This institute is furthermore reported[451] to be responsible for the Breakthrough Research programme (budget approximately EUR 63 million) and the National Security Technology Research Promotion Fund, under which the private sector is invited to apply for basic research that will contribute to future defence capabilities (budget approximately EUR 64 million).
- The Cabinet Office is in charge of Japan's economic security policy. One of the goals of this policy is to foster critical technologies such as artificial intelligence and quantum technologies[452], which may also be understood to refer more broadly to technologies with dual-use potential. This is implemented through the K Program (Key and Advanced Technology R&D through Cross Community Collaboration Program), which identified fifty technologies[453] as sensitive technologies. This programme aims to fill a gap with other funding programmes as it is concerned with technologies that can lead to the superiority and indispensability of Japanese technology, which may not receive sufficient funding if left solely to the mechanisms of the market economy, and which align for public needs. The K Program is being run in conjunction with the funding agencies JST (Ministry of Education, Culture, Sports, Science and Technology) and NEDO (METI), which together have a five-year budget of ca. EUR 3 billion for this purpose.

International dimension

The programmes run by the Japanese government to fund dual-use research, as outlined above, are not designed for international collaboration. There is no evidence of entry-points for foreign-based companies to benefit from any of the funding offered by these programmes.

Export control in Japan falls under the remit of the Ministry of Economy, Trade and Industry (METI), which issues export licenses according to two regimes[454]:

- List control: Arms and dual-use items that can be diverted to military use.
- Catch-all control: All items except those subject to the list control, food products, and timbers are subject to Catch-all control if it seems that they are to be involved in the development, design, manufacture, and storage of weapons of mass destruction and/or missiles.

It is the exporter themselves that judges whether the items are subject to either of these two forms of control, or not at all. Nevertheless, METI reserves the right to inform an exporter that they are subject to catch-all control.

---

[448] Japan Ministry of Defence (2024), 'Press Conference by Defense Minister Kihara on Tuesday, October 1, 2024, at 11:08 AM'.
[449] Kyodo News (2024), 'Japan to open U.S.-inspired defense tech research center in October'.
[450] Acquisition, Technology and Logistics Agency (2025), 'ATLA Research & Development'.
[451] Japan Press Weekly (2024), 'Gov't move to promote integration between gov't, industry, and academia creates dangerous path toward becoming a war-fighting nation'.
[452] Shiraishi (2024), 'Japan's Economic Security Policy'.
[453] Science Japan (2023), 'The Cabinet Office's K Program adds 23 various and advanced projects in its "2nd Vision" based on reports from JST/CRDS'.
[454] Japan Ministry of Economy, Trade and Industry (2021), 'Security Export Control'.

Republic of Korea[455]

Box 12: Awareness across the divide: Dual-use research in the Republic of Korea

The Korean dual-use research system emphasises clearly the importance of joint awareness and evaluation of projects between the government ministry that manages civilian research matters and that which is responsible for national defence. Proposals for defence research, for instance, require scouting for similar technologies in the civilian market.

Source: The author.

Policy background

Although the statutes of the Republic of Korea (ROK) make explicit reference to dual-use goods primarily in the context of foreign trade[456], the concept of '*[fostering] technological cooperation between the military and non-military sectors by promoting research and development of related technology'* is the foundational principle behind the Promotion of Technology Projects for Joint Civilian and Military Use Act[457] and has been so since this act was first promulgated in 1998[458]. ROK research policies that could be considered to fall under the category of dual-use R&I are therefore more properly seen through this, slightly broader, lens.

Against the backdrop of its geopolitical situation, policies and strategic plans of the ROK[459] make extensive reference to the need to bolster its national security and invest in developing new and emerging technologies. The government of ROK presently dedicates approximately EUR 3.5 billion from its domestic research and development budget to "national strategic R&D programmes"[460], with the ROK government aiming to follow the US Defense Advanced Research Project Agency (DARPA) model. The stated aim of the ROK defence ministry is to secure 5% of the global arms export market by 2027[461].

Funding of dual-use R&I

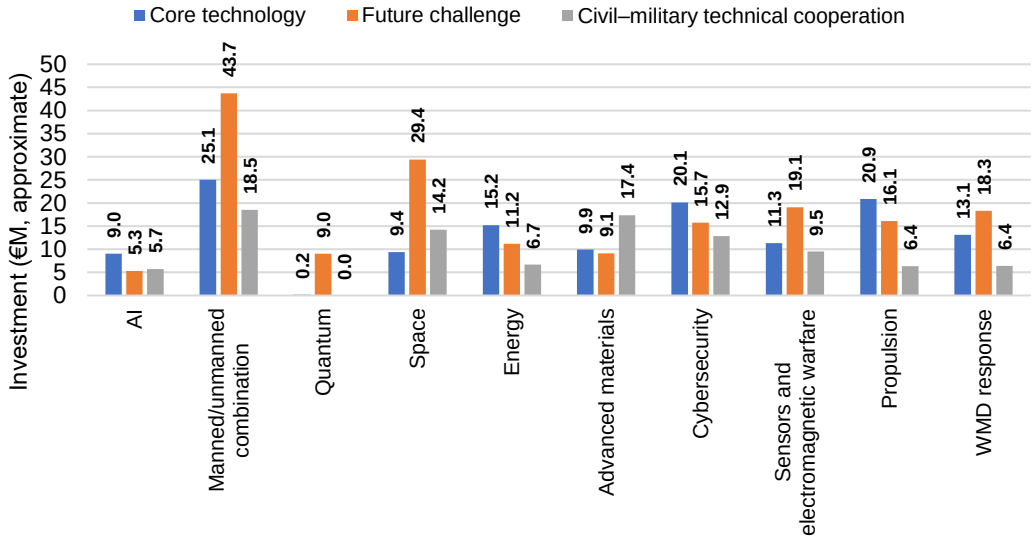
Funding for R&I projects in fields that could fall under the category of dual-use technologies is spearheaded by two ministries in the ROK, ostensibly split into research for civilian purposes and research for military and defence applications. The former is the purview of the Ministry of Science and ICT, as well as its related agencies, whereas the latter falls under the remit of the Ministry of National Defense and the Defense Acquisition Program Administration and is mainly executed under the legal framework of the Defense Acquisition Program Act[462].

In 2023 the ROK Ministry of National Defense launched the National Defense Science and Technology Basic Plan (2023–2027)[463]. This is a long-term political direction and promotion strategy that serves as a set of guidelines in the field of defence R&D. Building on the twelve fields identified by the Ministry of Science and ICT (MSIT) in 2022[464], it puts forth a set of ten strategic fields that are of significant importance to maintain national security, these being:[465] artificial intelligence, manned/unmanned combination[466], quantum technologies, space, energy, advanced

[455] The original financial numbers in this section were expressed in KRW; an approximate conversion is being made to EUR for the purposes of comparison across countries.
[456] Korea Legislation Research Institute (2003), Foreign Trade Act.
[457] Korea Legislation Research Institute (2018), Promotion of Technology Projects for Joint Civilian and Military Use Act.
[458] Due to a misprint there is a discontinuity in the history of the Act; for 1998–2011 refer to: https://elaw.klri.re.kr/eng_service/lawView.do?hseq=23680&lang=ENG
[459] ROK Ministry of Science and ICT (2022), 'Korea to announce national strategy to become a technology hegemon'.
[460] ROK Ministry of Science and ICT (2023), 'Taking a leap toward becoming a world-leading science and technology hub'.
[461] Sang-ho (2022), 'S. Korea aims for 5 pct share in global arms market by 2027', Yonhap News Agency'.
[462] Korea Legislation Research Institute (2024), Defense Acquisition Program Act.
[463] ROK Ministry of National Defence (2023), *National Defense Science and Technology Basic Plan (2023–2027)*.
[464] ROK Ministry of Science and ICT (2022), 'Korea to announce national strategy to become a technology hegemon'.
[465] The names of these technologies were machine-translated from Korean and may be inaccurate.
[466] This refers to the combination of manned and autonomous activities, particularly in the context of future battlefields.

materials, cybersecurity, sensors and electromagnetic warfare, propulsion technologies and weapons of mass destruction (WMD) response. Figure 16 gives an overview of existing ROK government investment in these fields as of 2023, when 24% (approximately EUR 97 million) was dedicated to what is labelled "civil–military technical cooperation." In the same year, the defence R&D budget (ca. EUR 3.5 billion, 9% of the ROK defence budget or 0.23% of GDP[467]), included ca. EUR 125 million (0.009% of GDP) allocated to civil–military technical cooperation.

Figure 16: Existing ROK government investment in different defence technologies as of 2023.



Source: ROK Ministry of National Defense, *National Defense Science and Technology Basic Plan (2023–2027)* (2023).

The National Defense Science and Technology Basic Plan emphasises that in the evaluation procedure for projects, it is essential to check whether technology that is being proposed for military applications has already been developed in the private sector. This is performed in coordination with the National Science and Technology Research Council (NST) under MSIT. The MSIT regularly surveys interested organisations[468] to discover new tasks for the civil–military cooperation projects in the context of strengthening simultaneously the industrial competitiveness and the national defence capability of the ROK. Strictly defence-oriented basic research is mostly conducted in-house by the Agency for Defense Development, with the ROK defence industry ultimately being responsible for manufacturing.

International dimension

In its master plan for 2024–2028 aimed at developing critical and emerging technologies, MSIT identified the need for stronger international cooperation with "like-minded countries",[469] although it is not clear how this will translate to the possibility, or otherwise, for foreign entities to cooperate with ROK partners when applying for funds for dual-use R&I. The National Research and Development Innovation Act[470] and the Defense Technology Security Act[471] contain provisions for safeguarding against the leakage, including of knowledge, expected to cause significant loss in

[467] World Bank, 'GDP (current LCU) - Korea, Rep.'.

[468] ROK Ministry of Science and ICT (2023),년도 착수 민군겸용기술개발사업 기술수요조사 공고 [machine translation: 2024 Commencement of Civil-Military Technology Development Project Technology Demand Survey Announcement].

[469] ROK Ministry of Science and ICT (2024), 'MSIT Unveils First Master Plan for Developing Critical and Emerging Technologies (2024-2028): A Blueprint for National S&T Sovereignty'.

[470] Korea Legislation Research Institute (2023), National Research and Development Innovation Act.

[471] Korea Legislation Research Institute (2020), Defense Technology Security Act.

technical or property value. Under these acts, the relevant ministry may classify tasks that satisfy this criterion; researchers conducting such projects should establish security measures in advance. Imports and exports of dual-use goods more broadly are, as mentioned earlier, governed by the Foreign Trade Act[472].

4.2.3. Middle-East

Israel[473]

Box 13: Fast track: Facilitating the uptake of new dual-use technologies by Israel

The INNOTAL programme aims to find and implement innovative technologies for the Israeli Defense Forces. Several challenges are published across a number of fields; funding is initially awarded for pilot projects which, if successful, progress to full implementation.

Source: The author.

Policy background

The economy of Israel is highly dependent on its high-tech industry, accounting for just less of one-fifth of its GDP[474], and the defence sector, which accounted for ca. 10% of Israeli exports[475] in 2018. This country has a strong and well-developed system of funding R&I, including programmes that cater specifically for dual-use technologies across all the stages of their life cycle from fundamental research through to the pre-product stage.

Funding of dual-use R&I

The primary state actor involved in funding dual-use R&I in Israel is the Israel Innovation Authority (IIA), through its Technological Infrastructure Division, which runs the MEIMAD[476] programme[477]. This programme is a joint venture of the IIA, the Israeli Ministry of Finance, and the Israeli Ministry of Defense through its Administration for the Development of Weapons and Technological Infrastructure. MEIMAD supports the development of innovative dual-use technological solutions for the defence and commercial markets through three sub-programmes[478]:

- *Academia***:** This programme incentivises applied research with innovative technological feasibility originating in academia and its advancement to the stage at which an Israeli company will adopt it to develop as a commercial product. This programme is further split into funding for academic researchers, whether by themselves or partnered with a corporation, and a special category for pharmaceutical knowledge transfer.
- *Industry***:** The programme is intended to enable a company to absorb the knowledge developed by an academic institution and to adapt it to its needs for developing novel products. It facilitates transfer of knowledge from an academic institution (which can be non-Israeli) to a corporation, primarily via repetition of the research results, their validation, adaptations to industrial conditions, and industrial application.
- *Pre-product:* This programme aims to fund the development of groundbreaking pre-product technologies with dual-use potential.

The overall goal of MEIMAD is to promote the exploitation of dual-use technologies in both military and commercial applications, both to contribute to national security and to help realising the

[472] Korea Legislation Research Institute (2003), Foreign Trade Act.
[473] The original financial numbers in this section were expressed in NIS; an approximate conversion is being made to EUR for the purposes of comparison across countries.
[474] Israel Innovation Authority (2023), *2023 Annual Report: The State of High-Tech*.
[475] Israel Ministry of Defense, 'Advancing Defense Exports'.
[476] This word is a transliteration of the Hebrew word "מימד," which literally means measurement.
[477] Israel Innovation Authority, 'Leveraging R&D for Dual Use Technologies – MEIMAD'.
[478] Israel Innovation Authority (2021), 'Activities of the Israel Innovation Authority's Divisions'.

economic potential of innovations by providing an opportunity to transfer military capabilities to the civilian market and vice versa. The IIA also operates programmes that fund dual-use R&I on behalf of other government entities. Together with the Ministry of National Security, it runs a programme[479] that supports pilot projects related to homeland security. Such projects are expected to be ready for a trial deployment without any further significant research and development.

The Directorate of Defense, Research and Development (DDR&D), Dual-Use Unit within the Israeli Ministry of Defense promotes technologies, including robotics, artificial intelligence, drones, photonics, quantum technologies, and cyber-defence, with clear dual-use potential. It serves to bring together the Israeli security forces, government bodies, private investment companies, and corporations. Separately from IIA and MEIMAD, the DDR&D runs a number of programmes:

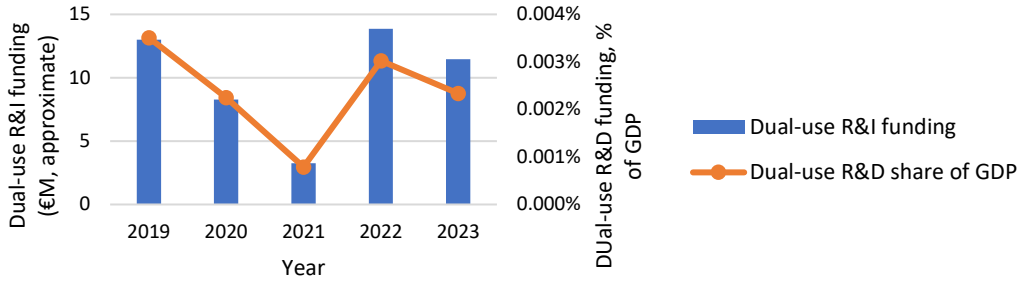
- INNOFENSE maintains a list of defence challenges with the aim of locating startup companies able to develop technological solutions for them. The programme targets early-stage technologies[480] (TRL 3–5) and disburses approximately €50k of non-dilutive funding[481] per project. The companies retain full intellectual property rights and includes business mentorship.
- INNOTAL, operated by the Israeli Innovation Institute, aims to identify groundbreaking Israeli technologies and integrate them into the Israeli Defense Forces through its technology and logistics directorate. This programme emphasises relatively mature technologies[482] (TRL 5–7). Similarly to INNOFENSE[483], this programme disburses approximately EUR 50,000 of non-dilutive funding per project, and the companies retain full intellectual property rights.
- MAFAT Challenge[484] which is a series of prize competitions in the field of data science open to the general public, academia, and the industrial sector.

A key feature of these programmes is that they facilitate uptake of successful results by entities such as the Ministry of Defense, and the Israeli Defense Force. For example, INNOTAL includes a commitment by the authorities to decide on a full implementation of the technology on the basis of the results of the pilot projects it funds. Through an additional programme called the Green Lane Track, startups are encouraged to present innovative technological solutions directly to the Israeli Ministry of Defense and the IDF, with any subsequent commercial engagement being under simplified conditions, e.g., through exemption of ISO requirements and expedited payment terms.

The financial commitment of the IIA to dual-use research (Figure 17) from 2019 to 2023 averages to an annual spend of ca. EUR 10 million (2019: EUR 13 million[485], 2020: EUR 8.3 million[486], 2021: EUR 3.3 million[487], 2022: EUR 14 million[488], 2023: EUR 11 million[489]), or about 0.002% of the GDP of Israel[490] (0.001%–0.004% over the same period). Figures for the Ministry of Defense are hard to come by; it has reportedly[491] disbursed approximately EUR 155 million in 2024 (0.03% of GDP) in activities related to startups, a fivefold increase over the previous year. These figures contrast with the current military expenditure of approximately 5% of GDP[492].

[479] Israel Innovation Authority, 'Support Program for Innovation in Selected Fields – Homeland Security (HLS)'.
[480] Directorate of Defense, Research and Development, 'INNOFENSE'.
[481] This refers to funding that is given to a company without the company giving up equity, i.e., a stake in its ownership, in return.
[482] Directorate of Defense, Research and Development, 'MAFAT For Startups'.
[483] InnoTal, טכנולוגיות ישראליות לצה"ל (machine translation: Israeli Technologies for the IDF).
[484] Directorate of Defense, Research and Development, 'MAFAT For Startups'.
[485] Israel Innovation Authority (2020), *Israel Innovation Authority's 2019 Innovation Report*.
[486] Israel Innovation Authority (2021), *2021 Annual Report: The State of High-Tech*.
[487] Israel Innovation Authority (2022), *2022 Annual Report: The State of High-Tech*.
[488] Israel Innovation Authority (2024), *2024 Annual Report: The State of High-Tech*.
[489] Israel Innovation Authority (2023), *2023 Annual Report: The State of High-Tech.*
[490] World Bank, 'GDP (current LCU) – Israel'.
[491] Frantzman (2024), 'Israel's Ministry of Defense quintupled start-up funding in last year'.
[492] World Bank, 'Military expenditure (current LCU) – Israel'.

Figure 17: Israeli dual-use R&I funding allocated through the Israel Innovation Authority, and the share of the GDP it represents, between the years 2019 and 2023.



Source: Estimation done by the author, based on data sources presented above.

International dimension

The Israel Innovation Authority maintains a comprehensive list of bilateral programmes with countries from around the world[493] supporting collaborative research by Israeli and foreign entities or individuals. Although no evidence was found for programmes tailored to dual-use research in particular, many of these programmes fund all technology fields[494]. The MEIMAD programme includes an international component but appears to be limited to collaborations between Israeli entities and foreign academics.

Export control in Israel is in the remit of the Export Control Agency of the Ministry of Economy and Industry.[495] Licenses are applied for by individuals engaged in the export (including re-export) of listed technologies or services.

4.2.4. Europe

Finland

Box 14: Catering to the world: Internationalisation for economic growth in Finland

The Finnish dual-use and defence sectors rely on exports for a sizeable portion of their revenues. This international quality to the market means that companies attract both international customers and foreign venture capital, to the benefit of the Finnish economy.

Source: The author.

Policy background

The defence industry in Finland is a strong exporter; typically, 40% to 60% of its revenues come from exports[496]. Around the same time as the accession of Finland to NATO, the support of funding for dual-use R&I became more visible. Tesi, the Finnish national investment company, has reported that dual-use companies show the strongest growth in the entire defence sector in the past two decades[497], as illustrated in Figure 18. This realisation is by no means unique. In its published views on the priorities of the forthcoming European Commission multiannual financial framework, Business Finland, a public sector organisation that supports Finnish companies, states

[493] Israel Innovation Authority (2025), 'International Collaborations'.
[494] Israel Innovation Authority (2025), 'International R&D and Pilot Collaborations – 2025'.
[495] Israeli Ministry of Economy and Industry (2023), 'Export Control Agency'.
[496] Association of Finnish Defence and Aerospace Industries (2021), 'PIA Key Facts & Figures 2021'.
[497] Tesi (2024), 'Finnish defence industry growing strongly, investors eyeing dual-use products in particular'.

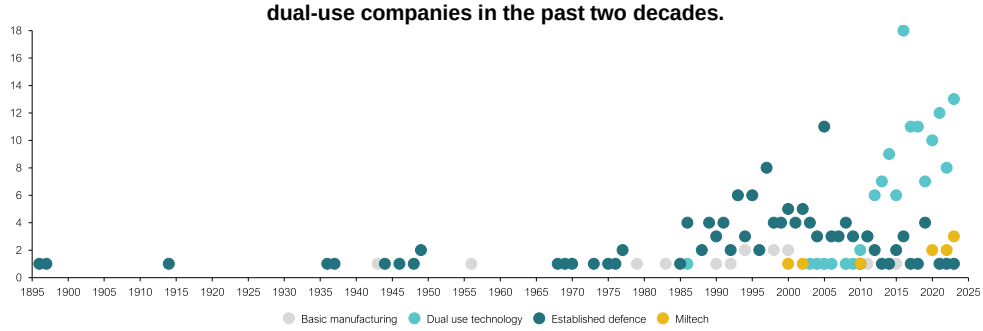
clearly that "*development of dual use technologies should be integrated into the programmes in which the related civilian applications are developed*."[498]

From an economic perspective, it is instructive to note that dual-use technology and military technology firms are growing quickly (median sales compound annual growth rates of 6% over the five years to 2024) and with an accelerating growth rate[499].

Funding of dual-use R&I

The main lines of responsibility for government funding R&I in Finland are assigned through a Government Standing Order. Responsibility for the research, development and innovation policy as well as technology policy is split between the Ministry of Economic Affairs and Employment and the Ministry of Education and Culture for matters that concern science policy. The Ministry of Defence, in turn, is focused on R&I related specifically on capabilities and technological niches that are not served by more mainstream R&I activities. The Research Council of Finland (2025 budget approximately EUR 515 million[500]) funds dual-use research[501], so long as dual-use and ethical aspects are identified and considered in proposals. Dual-use R&I activities in the private sector are funded by Business Finland through its Defense and Digital Resilience programme[502].

Figure 18: Growth in the number of Finnish defence companies since the 1890s; note the rapid growth of dual-use companies in the past two decades.



Source: Tesi, *Defence: Market study on Finnish military product and dual-use companies* (2024).

Venture-capital funding is an important aspect of the dual-use funding landscape in Finland, accounting for approximately 37% of funding awarded to dual-use technologies[503]. In fact, between 2015 and 2024, 163 investment rounds were identified in the defence industry in Finland (totalling ca. EUR 1.1 billion)[504], almost all of which were made in dual-use companies. In common with other markets, the transaction value peaked sharply in 2022, subsequently dropping to pre-COVID levels. Quite some insight can be gleaned from a snapshot of the nature of investment going into various parts of the Finnish defence industry (Figure 19). Venture capital funding is in fact one of the primary sources of finance for dual-use technology companies and, to a lesser extent, military technology companies in Finland. The link between venture capital and dual-use companies in Finland is very strong. The data shows that a total of 368 companies work in the defence industry, out of which 54 were backed by venture capital[505]. From this latter cohort of companies, 50 (93%) were identified as dual-use technology companies[506]. The same data reveals that five of the 143 dual-use firms were under foreign ownership, a share (4%) significantly lower than the overall share of foreign-owned firms in the defence market (12%). The majority of firms in the defence

[498] Business Finland (2024), 'Business Finland's views on the main priorities in EU RDI programmes MFF 2028-2034'.
[499] Tesi (2024), Defence: Market study on Finnish military product and dual use companies.
[500] Research Council of Finland (2024), 'Research Council of Finland to fund wide range of excellent research in 2025'.
[501] Research Council of Finland, 'Funding criteria and policies'.
[502] Business Finland, 'New global competitive edge from comprehensive digital security and defence'.
[503] Tesi (2024), Defence: Market study on Finnish military product and dual use companies.
[504] *Ibidem*.
[505] *Ibidem*.
[506] *Ibidem*.

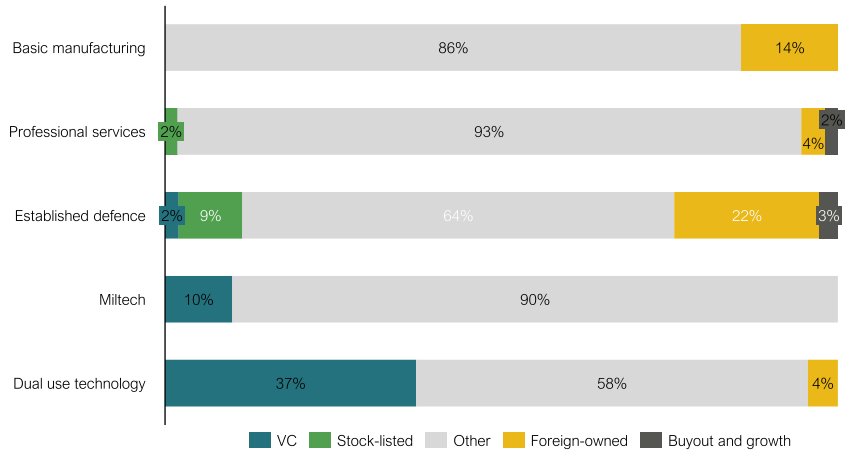
sector, across all areas, are under Finnish ownership with no identified equity investments (labelled "Other" in Figure 19).

International dimension

The defence industry in Finland relies heavily on exports for approximately half of its revenues (43% in 2020[507]). Out of the 144 dual-use and military technology companies operating in Finland in 2024[508], ten were identified as being foreign-owned. The same data shows that these 144 companies constitute almost 40% of the firms operating in the Finnish defence sector. Financial incentives to assist business in performing dual-use R&I do not seem to be limited to Finnish-owned businesses; for instance, Business Finland targets foreign companies operating in the defence and dual-use sectors that wish to invest in Finland. Export control in Finland is the responsibility of the Ministry for Foreign Affairs[509] in line with the appropriate EU regulations.

No evidence can be found for restrictions imposed on foreign researchers being involved in dual-use research in Finland. However, Principal Investigators leading research projects involving, e.g., dual-use products "must explain in sufficient detail in the [research] application how these have been taken into account"[510].

Figure 19: Sources of funding or ownership for companies operating in the defence industry in Finland. There is a strong link between venture capital and dual-use technology companies.



Source: Tesi, *Defence: Market study on Finnish military product and dual-use companies* (2024).

United Kingdom[511]

Box 15: Fostering trust and making strong connections: The UK dual-use R&I system

The United Kingdom operates the Trusted Research system. This is a set of guidelines that apply to all aspects of the dual-use research ecosystem across both academia and industry, ensuring that all actors are aware of, and operate in conformity with, applicable legislation.

The United Kingdom places significant emphasis on the transfer of research and innovation between the civilian and the defence markets. The jHub Defence Innovation Accelerator is intended to bring civilian innovation to the defence market, whereas Ploughshare is set up to create spin-outs that turn government-owned intellectual property into commercial products.

Source: The author.

[507] Association of Finnish Defence and Aerospace Industries (2021), 'PIA Key Facts & Figures 2021'.
[508] Tesi (2024), Defence: Market study on Finnish military product and dual use companies.
[509] Ministry for Foreign Affairs of Finland, 'Export control'.
[510] Research Council of Finland, 'Research ethics'.
[511] The original financial numbers in this section were expressed in GBP; an approximate conversion is being made to EUR for the purposes of comparison across countries.

Policy background

The United Kingdom (UK) has an advanced and diversified R&I system, encompassing the public, private, and academic sectors. Research programmes that could be classified as dual-use consist of a mix of funding types, including grants aimed at funding bottom-up research; themed competitions that are more top-down; calls for procurement; loans; and venture capital funds, both government and private. Several policy documents guide the UK government's approach towards defence and dual-use R&I:

- The UK Defence and Security Industrial Strategy[512], published in 2021, identifies opportunities for development of and access to dual-use technologies. It aims to exploit the linkages between the commercial market, which drives most technological advances, and the defence market, particularly in the context of the Defence Innovation Priorities[513] identified by the Ministry of Defence (MOD) in 2019. This strategy is presently under review and expected to be updated in spring 2025 under the guise of the Defence Industrial Strategy[514].
- The Science and Technology Framework[515], published in 2023, identifies five technologies that are critical for the UK according to eight criteria, including national security and defence. These are artificial intelligence, engineering biology, future telecommunications, semiconductors, and quantum technology. This list is subject to annual review, although such reviews are not expected to make material changes to the list. A national strategy or vision document has been published for each technology, with all these strategies making mention of dual-use issues; these documents lie beyond the scope of this chapter.
- The Integrated Review Refresh of 2023[516], updating a 2021 policy document, reiterates the critical nature of the same five technologies identified previously and reaffirms the importance of the UK's "own, collaborate, access" framework[517] which aims to ensure that the UK has a clear route to assured access for each of these critical technologies, including by acquiring critical science and technology from elsewhere.

Funding of dual-use R&I

The lynchpin of the UK dual-use R&I funding programmes is the Ministry of Defence (MOD), which engages in the making of policies, running of programmes, and operation of agencies across both defence-only and dual-use topics. The MOD collaborates extensively with the private sector, other departments within the UK government, and academia. Aside from the Defence Academy of the United Kingdom[518], which is run by the MOD, academic institutions have access to Centres for Doctoral Training funded directly by the MOD[519]. The key entities are:

- The Defence Science and Technology Laboratory (DSTL), which is the MOD's science and technology organisation, performs scientific research with military applications. The Defence and Security Accelerator is part of DSTL and engages with the private sector, including SMEs, on small projects that could have military use through open calls for funding that target all TRLs[520] and had a 2023–2024 budget of around EUR 62 million[521]. This compares to an overall

[512] UK Ministry of Defence (2021), *Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors*.
[513] UK Ministry of Defence (2019), *Defence Innovation Priorities*.
[514] UK Ministry of Defence (2024), Defence Industrial Strategy - Statement of Intent.
[515] UK Department for Science, Innovation and Technology (2023), *The UK Science and Technology Framework.*
[516] UK Cabinet Office (2023), *Integrated Review Refresh 2023: Responding to a more contested and volatile world*.
[517] UK Cabinet Office (2021), *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*.
[518] UK Ministry of Defence, 'Defence Academy of the United Kingdom'.
[519] UK Ministry of Defence (2024), 'Ministry of Defence funds 2 new Centres for Doctoral Training'.
[520] UK Ministry of Defence (2019), 'The Defence and Security Accelerator'.
[521] UK Ministry of Defence (2024), *DASA Annual Review 2023-2024.*

UK government spend on R&D of approximately EUR 18 billion in 2022[522] (DSTL share approximately 0.33%) and corresponds to approximately 0.002% of the UK GDP[523].

- The jHub Defence Innovation Accelerator[524], which focuses on harnessing dual-purpose technology and has a particular interest in repurposing high TRL products and services from areas that do not traditionally have a defence focus.
- Ploughshare was launched by the MOD in 2005 to turn government-developed and owned intellectual property into commercial products and solutions by negotiating license agreements with the private sector and creating spin-outs.
- The National Security Strategic Investment Fund is the UK government's Venture Capital fund for dual-use and defence technologies. As of June 2023, NSSIF had commitments for approximately EUR 263 million in investments, together with co-investments totalling approximately EUR 860 million from private sector[525].
- The Advanced Research and Invention Agency (ARIA) and UK Research and Innovation (UKRI) are broad-spectrum agencies that fund projects across all sectors of technology and TRLs, with UKRI (total budget approximately EUR 30 billion for 2022–2025[526]) focusing on lower TRLs than ARIA (total budget approximately EUR 960 million over the period to 2025–2026[527]).
- A network of Catapults is operated by UKRI that also serve dual-use goals by providing testbeds and expertise that projects, including in defence, can tap into.

Complementing public-sector investments in defence and dual-use technologies in the UK is a strong venture-capital sector. Between 2014 and 2023, there were a reported 470 equity deals in these sectors amounting to ca. EUR 1.4 billion in total; these contrast with a total of ca. EUR 525 million in government grants awarded to these sectors over the same time period, spread over 1411 grants[528]. In common with other markets, defence and dual-use private venture capital in the United Kingdom peaked in 2022 and decreased sharply in 2023 to return to pre-COVID levels.

International dimension

International aspects of dual-use R&I are covered thoroughly in the UK system:

- The Export Control Joint Unit (ECJU) administers the UK's system of exports and licensing for military and dual-use items. It maintains guidelines[529] on export controls for academic research.
- The Research Collaboration Advice Team is meant to be the first point of contact and a trusted source for advice on identifying and mitigating risks to international research collaborations, including export controls, protection of intellectual property, reputation and values.
- The Academic Technology Approval Scheme, which is administered by the Foreign, Commonwealth and Development Office, applies to certain foreign students and researchers who want to study or conduct research in specific sensitive fields in the UK.
- Trusted Research is a scheme operated by the UK National Protective Security Authority and UK National Cyber Security Centre that provides guidance to researchers, university staff and

[522] UK Office for National Statistics (2024), 'Research and development expenditure by the UK government: 2022'.
[523] World Bank, 'GDP (current LCU) - United Kingdom'.
[524] jHub Defence innovation, available at: https://www.gov.uk/government/organisations/jhub-defence-innovation.
[525] UK Parliament (2023), 'National Security Strategic Investment Fund: Question for Department for Business and Trade'.
[526] UK Research and Innovation (2023), '2022-23 — 2024-25 budget allocations for UK Research and Innovation'.
[527] UK Parliament (2022), 'Advanced Research and Invention Agency'.
[528] Whorwood, Robinson, and Hyde (2024), 'UK Defence Tech 2024: Advancing National Security through Innovation'.
[529] UK Export Control Joint Unit (2024), Export controls applying to academic research.

funding organisations to keep sensitive research and intellectual property secure from theft, misuse or exploitation. UKRI operates the related Trusted Research and Innovation scheme.

- The National Security and Investment Act[530], which came into force in January 2022, gives the UK government powers to scrutinise and intervene in business transactions (such as takeovers) to protect national security.

4.2.5. North Atlantic Treaty Organisation

Background

The primary goal of North Atlantic Treaty Organisation (NATO) when commissioning R&I is typically to develop and procure defence capabilities. Nevertheless, it is clear that some knowledge or technologies will fall in the category of dual-use items, and this is appropriately reflected in the make-up and strategy behind NATO's main R&I funding programmes.

Funding of dual-use R&I

One of the most open funding programmes run by NATO is Science for Peace and Security[531] (SPS), which allows participation by NATO member states in collaboration with non-NATO partner countries on the basis of research, innovation, and knowledge exchange; the focus of SPS is on the lower end of the TRL scale. The SPS Programme is seen by NATO as providing a means for non-military communication amongst scientists and experts. Projects are considered for funding in a number of key priority areas, including environment, climate change, and security; energy security, innovation and emerging disruptive technologies; counterterrorism; chemical, biological, radiological, and nuclear and explosive hazard management; defence against hybrid threats; resilience; critical underwater infrastructure; cyber defence; strategic foresight; and human and social aspects of security. The detailed breakdown of these areas includes topics of civilian, military, and dual-use interest. The stated aim of SPS is, nevertheless, to enhance "security-related civil science and technology to address emerging security challenges and their impact on international security,"[532] rather than dual-use research. SPS multi-year research projects can benefit from up to about EUR 400,000 in funding. The most recent budgetary figures that can be found are from the 2020 Annual Report[533], when the annual expenditure for SPS stood at EUR 11.8 million.

The recently launched Defence Innovation Accelerator for the North Atlantic[534] (DIANA) is explicitly aimed at increasing the dual-use innovation capability across NATO. This programme targets technologies with TRL above 6 and is primarily intended for dual-use tech startups which already have a fair outlook of the civilian market but wish to explore opportunities in the defence sector. Companies accepted for funding are awarded EUR 100,000 for the first six months and up to EUR 300,000 for an additional six months following a competitive selection. In 2023 NATO also launched the NATO Innovation Fund[535], a EUR 1 billion venture capital fund that can invest directly in 24 NATO countries. This fund operates primarily in the deep-tech ecosystem and contemplates investments of up to EUR 15 million for the initial round of funding. Amongst its primary objectives is to help startups identify adoption pathways to ensure integration of emerging technologies in the Allied defence and security infrastructure.

The Defence Against Terrorism Programme of Work (DAT POW)[536] was launched by NATO in 2004. With an initial focus on technological solutions to mitigate the effects of terrorist attacks, the programme has since widened its scope to support comprehensive capability development. This programme primarily focuses on finding solutions that can be deployed in the short term and that

[530] UK Cabinet Office (2020), National Security and Investment Act 2021.
[531] NATO (2023), 'Science for Peace and Security Programme'.
[532] NATO (2023), 'SPS Grant mechanisms'.
[533] NATO (2021), *SPS Programme Annual Report 2020*.
[534] NATO, DIANA, available at: https://www.diana.nato.int/.
[535] NATO, The NATO Innovation Fund, available at: https://www.nif.fund/
[536] NATO (2024), 'Countering terrorism'.

respond to the military needs of NATO. Through this programme, NATO is consulting with stakeholders from industry, the military and academia to explore how innovative technologies can be used in the fight against terrorism. It is not clear what the budget allocated to DAT POW, the size and duration of projects, or the eligibility criteria for participation are.

4.3. A comparison of dual-use R&I funding programmes

The dual-use funding programmes explored in this chapter differ markedly from each other in their underlying philosophy, how they operate, what controls they impose, etc. The present section rationalises this complex landscape through direct comparisons between the programmes and also extracts the common themes that underlie them.

4.3.1. Rationale

The rationale used to justify funding for dual-use R&I falls primarily in the economic or strategic camps, with many programmes making an argument based on a combination of the two.

First, an *economic* justification is deployed in some instances:

- In Finland, being a relatively small country, the domestic defence market is rather small, making the export market an important part of its dual-use ecosystem.
- The Republic of Korea describes its intention to pursue economic growth, e.g., by becoming one of the top defence exporters globally.

Second, a *strategic* argument, whether defensive or offensive, is often made:

- Israel, Japan, the Republic of Korea, and (to some extent) NATO allude to the geopolitical situation as a principal factor in motivating a dual-use and, more broadly, defence ecosystem.
- The People's Republic of China and the United States of America, as well as the United Kingdom, emphasise the importance of R&I to pursue or maintain technological superiority.

The distinction between arises mostly in the political narrative used to justify funding dual-use R&I. More than a theoretical distinction, this distinction is likely to be particularly important in designing dual-use funding programmes in the EU, where several countries with varied constitutional backgrounds are involved, including neutral countries for which strategic arguments may not apply.

4.3.2. Policy

All the surveyed dual-use systems have a mixture of funding mechanisms that they deploy to fund dual-use R&I. To a certain extent, funding is generally available both for bottom-up exploratory research, e.g., through more conventional research funding programmes, and in a top-down fashion for specific key technologies, e.g., through targeted pre-commercial technology acquisition programmes.

Bottom-up programmes, particularly those targeting very early-stage research, are essential for developing ideas that may eventually give rise to innovative dual-use technologies. Considerations for dual-use R&I in such funding programmes seems to be the exception, however. One key example is the Research Council of Finland, which disburses funding across all fields of study whilst explicitly allowing for dual-use research to be conducted subject to adequate considerations being made by the principal investigator in their research proposal.

The strategic thinking guiding top-down programmes varies highly from one programme to another. The PRC, Republic of Korea, and UK, for example, exhibit a "whole of government" approach, with certain technologies being identified as critical and in need of development centrally, e.g., through a government-wide strategy or policy document. There is some evidence that this strategy could yield dividends in the short term, e.g., with the PRC gaining global leadership in the field of quantum

communication despite having entered the field much later than other regions. Conversely, dual-use R&I in the US is in the remit of several departments and agencies, each independently setting their own technological priorities. The US provides evidence that such an approach, at least in the long term, could lead to leadership being asserted across a very broad swathe of technologies.

An interesting case study for the EU context is that of NATO. Despite being funded by all its member states in line with their own defence priorities, NATO centrally administers R&I funds according to the priorities of the organisation as a whole, although ultimately in agreement with its allies. This model strikes a balance between ensuring that the interests of each NATO member are represented, and bringing these interests closer.

4.3.3. Internationalisation

The funding systems surveyed deal with internationalisation both through the possibility to import dual-use knowledge, technology, and investment, as well as to export dual-use products.

Foreign participation

Participation of foreign individuals or entities in dual-use R&I funding programmes can itself be seen from different perspectives. First, funding programmes may allow or forbid foreign companies from benefiting by participating in projects. The UK is on the open end of the spectrum in this sense, with the Defence and Security Accelerator being in principle open to companies from anywhere so long as they satisfy specific criteria. At the other end of the scale, in Japan there do not seem to be any entry points for foreign companies to benefit from dual-use R&I funds.

Second, foreign researchers or academic institutions can be seen as one way of importing knowledge into an ecosystem. In the domain of dual-use R&I, the UK is cautiously open to foreign researchers, putting in place safeguards to ensure that dual-use technology is not leaked, whereas the US typically restricts project personnel to US citizens or permanent residents. Israel welcomes collaboration with foreign academic entities in some programmes, but places emphasis on commercialisation by Israeli companies.

Export regulations

Export regulations recur as one of the key issues faced by companies operating in the dual-use technology space. International regulations on dual-use technologies are always to be followed, but the implementation of these regulations, as well as any additional safeguards applied at the national level, varies from one country to the next. In some countries, e.g., the US, the responsibility for export controls of different technologies falls under different ministries or departments, potentially creating a patchwork of regulations. Others, e.g., the Republic of Korea, regulate everything through a central entity, streamlining the process.

4.3.4. Fragmentation

Another important aspect of any system of dual-use funding programmes is its level of fragmentation, specifically in terms of the number and kind of different funding agencies or similar entities that support or regulate it. This is one of the aspects which exhibited greatest variety amongst the surveyed systems as highlighted next.

- Segregation by type of entity, e.g., commercial or academia. Dual-use research in Japan falls under the remit of the Ministry of Economy, Trade and Industry, particularly for startups or SMEs; the Ministry of Defence, especially for projects run within academia; and the K Program, which funds R&I in several technologies identified as sensitive technologies by the government.
- Segregation by nature of work, e.g., dual-use or strictly defence. In the Republic of Korea, much dual-use research is administered by the Ministry of Science and ICT and the Ministry of National Defense, which coordinate to examine of proposals for funding that are neither strictly civilian nor strictly defence in nature.

- Segregation by TRL. NATO funding for dual-use research has a particularly simple landscape, being divided primarily into the Science for Peace and Security programme for low-TRL projects and the Defence Innovation Accelerator for the North Atlantic for high-TRL projects. To a considerable extent, Finland and Israel follow similar models.
- More complex landscapes. The United Kingdom and the United States of America each have a large system of funding agencies, business or technology accelerators, national laboratories or other facilities, and defence technology acquisition programmes.

These divisions and their descriptions are meant to be interpreted loosely, since it is often difficult to delineate strictly between funding programmes in the same ecosystem as well as to compare between ecosystems.

4.3.5. Bridge-building

One of the key reasons why several dual-use R&I funding programmes exist in the first place is to allow for bridges to be built between the civilian and defence markets. There is considerable added value to be gained by allowing technologies that are being primarily for the civilian market to be adopted for use in military contexts, or vice versa.

Some of the funding programmes discussed in this chapter are designed to exploit the synergies between defence and civil R&I. A few examples are:

- The Japanese government which, instead of only defining its defence needs and looking for appropriate technology providers, tasked the Ministry of Economy, Trade and Industry with curating a list of startups that may be in possession of dual-use technologies and meeting them to get a better understanding of their technologies and how they can be applied to defence.
- The Military–Civilian Fusion model employed by the People's Republic of China, which places no distinction between research performed for civilian or military purposes, thus allowing ideas and facilities to be shared between these two domains.
- The Ploughshare initiative of the United Kingdom, which takes government-funded inventions, often originating in defence laboratories, and incubates or licenses them to industry.
- The NATO Defence Against Terrorism Programme of Work is specifically aimed at identifying civilian solutions that can be migrated to the military.

Depending on the local context, scouting for innovations, particularly in academic institutions with the aim of bringing research conducted therein to the defence market, may meet with resistance if not done sensitively, since it may be seen as impinging on two aspects of academic freedom, i.e., the freedom to pursue any subject topic and the freedom to publish results of research.

4.4. Observations

Several essential features can be distilled from the studied dual-use R&I funding systems around the world, which may inform the design and help guide the implementation of new funding programmes:

- Dual-use research funding systems are not incompatible with defensive-only or pacifist stances, as illustrated by the case of Japan, and could explicitly promote both economic development and national security, as illustrated in the case of the Republic of Korea in its desire to become one of the top defence exporters globally.
- Fostering a dual-use R&I ecosystem may benefit from financial support and other initiatives across a broad range of TRLs, from basic research – even if application-driven – through to pre-commercial procurement. A mixture of bottom-up and top-down strategies may be employed in a synergistic fashion. For example, whereas the Military–Civil Fusion model of the PRC, and the Research Council of Finland both support strong funding systems for research

across a broad spectrum of topics, the former additionally focuses on specific dual-use technologies in a top-down fashion. An interesting example of a top-down challenge-led programme in the case of multinational organisations is the NATO DIANA programme, where the challenges target the security and defence needs of the NATO as a whole, rather than its individual allies.

- Designing simple landscapes for dual-use funding programmes is possible, e.g., by splitting funding programmes according to TRLs rather than which camp (civilian, dual-use, or military) they are intended to cover; particular examples of this strategy are Finland, where low-TRL research is supported by the Research Council of Finland and higher TRLs and commercialisation by Business Finland; Israel, through its MEIMAD programme; and the NATO funding system.
- Even in countries that praise international cooperation, dual-use research is observed to be a more inward-looking activity, where the participation of foreign entities or researchers is somewhat limited by safeguards, as illustrated by the US and UK, and the bringing of knowledge into the country may be prioritised, as in the case of Israel.
- Export control may be a significant regulatory burden for private companies operating in the dual-use sector, particularly for SMEs; for example, the US has onerous requirements on export control that impinge also on foreign nationals. Evidence from the surveyed funding systems suggests that targeted support for SMEs, including fast tracks to procurement (e.g., by the DIU and DARPA in the US), simplified regulatory frameworks, and temporary exemptions from certain regulations, may contribute to the earlier adoption of new technologies, as in the case of Israel.

Finally, several funding systems include mechanisms that support the cross-fertilisation of civilian and military research as contributing to economic, national security, and technological objectives. This attitude is seen practically across the board in the systems surveyed in this chapter, including in the Military–Civilian Fusion model employed by China, the scouting of startups in Japan, and the obligation to check the civilian market for possible solutions to military challenges by the Republic of Korea.

Bibliography

Civil-defence synergies

Addionics (2024), 'Unlocking Market Opportunities with Dual-Use Technologies', https://addionics.com/blog/unlocking-market-opportunities-with-dual-use-technologies/.

Albrycht, I., 'Cyberthreats to the Science and Research Sector as a Challenge to National Security and Economic Competitiveness' [*upcoming publication*].

Albrycht, I., Antunes, D., Burian, W., Cederlöf, J., Gray, C., et al. (2024), 'Dual-use Technology – Cross-sector cooperation in the cyber security sector', Cybersec Forum, https://cybersecforum.eu/wp-content/uploads/2024/12/Dual-use-technology-%E2%80%93-cross-sector-cooperation-in-the-cyber-security-sector.pdf.

Albrycht, I., Gawron, Ł., Góra, M., Hampel, M., Krawczyk, M. et al. (2022), 'Country's Systemic Resilience in the Digital Era', The Kosciuszko Institute, 2022.

Appathurai, J. (2025), 'European Parliament Committee on Security and Defence In association with the Delegation for relations with the NATO Parliamentary Assembly'.

Bondar, K. (2025), 'How Ukraine Rebuilt Its Military Acquisition System Around Commercial Technology', Center for Strategic and International Studies, https://www.csis.org/analysis/how-ukraine-rebuilt-its-military-acquisition-system-around-commercial-technology.

Bonvillian, W. B. (2024), *Pioneering Progress: American Science, Technology, and Innovation Policy,* The MIT Press, Cambridge, Massachusetts.

Bower, F. (2024), 'Venture Capital Investment in US National Security', Chronograph, https://www.chronograph.pe/venture-capital-us-national-security/.

Checkpoint (2024), 'A Closer Look at Q3 2024: 75% Surge in Cyber Attacks Worldwide', https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/.

Congressional Research Service (2021), 'Defense Advanced Research Projects Agency: Overview and Issues for Congress', https://sgp.fas.org/crs/natsec/R45088.pdf.

Council of the European Union (2022), *Informal meeting of the Heads of State or Government: Versailles Declaration*, https://www.consilium.europa.eu/media/54773/20220311-versailles-declaration-en.pdf?utm_source=dsms-auto&utm_medium=email&utm_campaign=The+Versailles+declaration%2c+10+and+11+March+2022.

Council of the European Union (2023), 'Joint Declaration on EU-NATO Cooperation, 10 January 2023', Press release, https://www.consilium.europa.eu/en/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/.

Dewan, A. (2025), 'Ukraine and Russia's militaries are David and Goliath. Here's how they compare', CNN, https://edition.cnn.com/2022/02/25/europe/russia-ukraine-military-comparison-intl/index.html.

Draghi, M. (2024), *The future of European competitiveness: A competitiveness strategy for Europe*, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

European Commission (n.d.), 'EU Compliance Guidance for Research Involving Dual-Use Items'. https://trade.ec.europa.eu/consultations/documents/consul_183.pdf.

European Commission (2015), 'Open Innovation 2.0 and Horizon2020: Opportunities and Challenges', https://digital-strategy.ec.europa.eu/en/news/open-innovation-20-and-horizon2020-opportunities-and-challenges.

European Commission (2020), *PASAG report 2 -2020 – Dual-Use for Security*, DG Migration and Home Affairs.

European Commission (2022), 'Roadmap on critical technologies for security and defence', COM(2022) 61, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52022DC0061.

European Commission (2024), *White Paper on Options for Enhancing Support for Research and Development Involving Technologies with Dual-Use Potential*, https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_white-paper-dual-use-potential.pdf.

European Commission (2024), *Align, Act, Accelerate: Research, Technology and Innovation to boost European Competitiveness*, DG Research and Innovation, Publications Office of the European Union, Luxembourg, https://op.europa.eu/en/publication-detail/-/publication/2f9fc221-86bb-11ef-a67d-01aa75ed71a1/language-en.

European Commission (2024), *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness*, https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en.

European Commission (2025), *2025 Commission work programme*, https://commission.europa.eu/strategy-and-policy/strategy-documents/commission-work-programme/commission-work-programme-2025_en.

European Commission (2025), 'Press statement by President von der Leyen on the defence package', Press statement, https://ec.europa.eu/commission/presscorner/detail/sv/statement_25_673.

European Commission (2025), *Joint White Paper for European Defence Readiness 2030*, JOIN(2025) 120 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0120.

European Commission (2025), *Joint Communication on the European Preparedness Union Strategy*, JOIN(2025) 130 final, https://webgate.ec.europa.eu/circabc-ewpp/d/d/workspace/SpacesStore/b81316ab-a513-49a1-b520-b6a6e0de6986/file.bin.

European Commission (2025), 'European Commission concludes public consultation on the EU Startup and Scaleup Strategy', https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/european-commission-concludes-public-consultation-eu-startup-and-scaleup-strategy-2025-03-26_en.

European Parliament (2025), *Resolution on the Future of European Defence*, 2025/2565(RSP), https://www.europarl.europa.eu/doceo/document/RC-10-2025-0146_EN.html.

European Union (2022), *A Strategic Compass for Security and Defence*.

Fiott, D. (2014), 'The three effects of dual-use: Firms, capabilities, and governance', European Union Institute for Security Studies, https://www.files.ethz.ch/isn/182624/Brief_21_Dual_use.pdf.

Fiott, D., and Ketselidis, M. (2022), 'EU Civil-Defence Synergies: Understanding the Challenges and Drivers of Change', Armament Industry European Research Group.

Garcia, D. C. (2025), 'Keen Venture Partners raising €125 million to strengthen Europe's defence tech ecosystem', EU Startups, https://www.eu-startups.com/2025/01/keen-venture-partners-raising-e125-million-to-strengthen-europes-defence-tech-ecosystem/.

Grace, J., Egan, J., and Rosenbach, E. (2023), 'Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S.', Belfer Center for Science and International Affairs, Harvard Kennedy School.

Hähnel, M., (2024), 'Conceptualizing dual use: A multidimensional approach', *Research Ethics Review*, 1-23, https://doi.org/10.1177/17470161241261466.

ICEYE (2024), 'ICEYE and the Ministry of Defense of Ukraine sign a Memorandum of Cooperation', Press release, https://www.iceye.com/press/press-releases/iceye-strengthens-cooperation-with-the-ministry-of-defense-of-ukraine.

International Institute for Strategic Studies (2021), *The Military Balance 2021*.

Kushnerska, N. (2025), 'What to expect from Ukraine's defence innovation in 2025', The Kyiv Independent, Accessed 20 March 2025, https://kyivindependent.com/what-to-expect-from-ukraines-defense-innovation-in-2025/.

Marijan, B. (2022), 'Russia's War on Ukraine Is a Test Case for Future Conflict', Centre for International Governance Innovation, https://www.cigionline.org/articles/russias-war-on-ukraine-is-a-test-case-for-future-conflict/.

McSorley, T. D., Macenowicz, M., Maddison, M., and Yukins C. (2025), 'Information and Analysis on Legal Aspects of Procurement', *The Government Contractor*, 67(1).

Moretti, E., Steinwender, C., and Van Reenen, J. (2019), 'The Intellectual Spoils of War? Defence R&D, Productivity and International Spillovers', National Bureau of Economic Research.

Nagy, S. R. (2018), 'Geotechnology Meets Geopolitics: US-China AI Rivalry and Implication for Trade and Security.' *World Commerce Review*.

NATO (n.d.), 'Diana – Homepage', https://www.diana.nato.int/.

NATO (2021), 'Opening remarks by NATO Deputy Secretary General, Mircea Geoană, at the 4th European Cybersecurity Forum – CYBERSEC Brussels Leaders' Foresight 2021', https://www.nato.int/cps/en/natohq/opinions_182357.htm.

NATO (2022), *Charter of the NATO Defence Innovation Accelerator for the North Atlantic (2022).*

NATO (2024), '2024 DIANA Challenge Programme Call for Proposals', https://www.diana.nato.int/resources/site1/general/2024_challenge_programme_web.pdf.

NATO (2024), 'Resilience, civil preparedness and Article 3', https://www.nato.int/cps/en/natohq/topics_132722.htm.

Niinistö, S. (2024), *Safer Together – Strengthening Europe's civilian and military preparedness and readiness*, https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en.

Reding, D. F., and Eaton, J. (2020), 'Science & Technology Trends 2020-2030: Exploring the S&T Edge', NATO Science & Technology Organization.

Rekowski, M., Piekarz, T., Sztokfisz, B., Siudak, R., Albrycht, I. et al. (2020), 'Geopolitics of Emerging and Disruptive Technologies', The Kosciuszko Institute.

Schlueter, M., Giesener, M., Mayer, L., and Plummer, M. (2022), 'Closing the Defense Innovation Readiness Gap', BCG and MSC, https://securityconference.org/assets/02_Dokumente/01_Publikationen/222014_-_MSC_-_Defense_Innovation_Report_-_Single_-_vonline.pdf.

Sezal, M. A., and Giumelli, F. (2022), 'Technology Transfer and Defence Sector Dynamics: The Case of the Netherlands', *European Security* 31(4), 558-575, https://doi.org/10.1080/09662839.2022.2028277.

Swartz, D., and Brukardt, R. (2025), 'Creating a modernized defence technology frontier', McKinsey & Company, https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/creating-a-modernized-defense-technology-frontier.

Tusk, D. (2025), 'Security, Europe! [Speech]', https://polish-presidency.consilium.europa.eu/en/news/security-europe-message/.

UK Government (2024), '"National security is the foundation for growth" - Defence Secretary launches new strategy to boost UK jobs and growth', Press release, https://www.gov.uk/government/news/national-security-is-the-foundation-for-growth-defence-secretary-launches-new-strategy-to-boost-uk-jobs-and-growth.

Verizon (2024), '2024 Data Breach Investigations Report', https://bakotech.pl/upload/fileuploads/files/2024-dbir-data-breach-investigations-report.pdf.

Von der Leyen, U. (2024), 'Europe's choice: Political Guidelines for the Next European Commission 2024-2029', https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf.

Practical implementation of dual-use R&I

BAFA (2023), 'Manual - Export Control and Academia', https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_manual_export_control_and_academia.html.

Bauer, S., Brockmann, K., Bromley, M., and Maletta, G. (2017), *Challenges and good practices in the implementation of the EU's arms and dual-use export controls: A cross-sector analysis*, Stockholm International Peace Research Institute, https://www.sipri.org/sites/default/files/2017-07/1707_sipri_eu_duat_good_practices.pdf.

Beaucillon, C., and Poli, S. (2023), 'Special Focus on EU Strategic Autonomy and Technological Sovereignty: An Introduction'. *European Papers*, 8(2), 411-416.

Bertello, A., Ferraris, A., De Bernardi, P., and Bertoldi, B. (2022), 'Challenges to open innovation in traditional SMEs: an analysis of pre-competitive projects in university-industry-government collaboration', *International Entrepreneurship and Management Journal*, 18, 89–104. https://doi.org/10.1007/s11365-020-00727-1

Bordin, G., Hristova, M., Luque-Perez, E. (2020), *Horizon 2020-funded security research projects with dual-use potential: An overview (2014-2018)*, Joint Research Centre, Publications Office of the European Union, Luxembourg.

Bureau of Industry and Security (n.d.), 'Export Administration Regulations – Scope of the Export', https://www.bis.gov/regulations/ear/part-734/section-734.8/technology-or-software-arises-during-or-results-fundamental-research.

CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper', https://www.cesaer.org/content/5-operations/2023/202310-white-paper-keeping-science-open/20231018-white-paper-keeping-science-open.pdf.

Colussi, I. A. (2024), 'The evolution of the EU STC system', in Michel, Q., and Paile-Calvo, S. (dirs.), Vella, V. (ed.), *Elaborating a strategic trade system of dual-use items*, Service for Foreign Policy Instruments, Publication Office of the European Union, Luxembourg, https://op.europa.eu/en/publication-detail/-/publication/cfcac057-76f9-11ef-bbbe-01aa75ed71a1.

Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, L 124, https://eur-lex.europa.eu/eli/reco/2003/361/oj/eng.

Commission Recommendation (EU) 2019/1318 of 30 July 2019 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009, L 205/15, https://eur-lex.europa.eu/eli/reco/2019/1318/oj/eng.

Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, https://eur-lex.europa.eu/eli/reco/2021/1700/oj/eng.

Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment, L 335/99, https://eur-lex.europa.eu/eli/compos/2008/944/oj/eng.

Council of the EU (2024), Recommendation of 23 May 2024 on enhancing research security, C/2024/3510, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510.

DESCA (n.d.), 'Desca Model Consortium Agreement', https://www.desca-agreement.eu/desca-model-consortium-agreement/.

Directive 2009/43/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defence-related products within the Community, L 146/1, https://eur-lex.europa.eu/eli/dir/2009/43/oj/eng.

Draghi, M. (2024), *The future of European competitiveness: A competitiveness strategy for Europe*, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

EARTO (2024), 'EARTO Answer to EC Consultation on Technologies with Dual-use Potential', https://www.earto.eu/wp-content/uploads/EARTO-Answer-to-EC-Consultation-on-Technologies-with-dual-use-potential-Final.pdf.

European Commission (n.d.), 'TIM Dual-Use, Knowledge for Policy', https://knowledge4policy.ec.europa.eu/text-mining/tim-dual-use_en.

European Commission (n.d.), 'Horizon Dashboard – R&I Projects', https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard.

European Commission (n.d.), 'Horizon IP Scan'. https://intellectual-property-helpdesk.ec.europa.eu/services/horizon-ip-scan_en.

European Commission (n.d.), 'EUDIS: Spin-in Calls', https://eudis.europa.eu/eudis-tracks/spin-calls_en#:~:text=Spin%2Din%20calls%20allow%20for,civil%20EU%2Dfunded%20R%26D%20and.

European Commission (2021), 'EU Grants - How to handle security-sensitive projects', https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/how-to-handle-security-sensitive-projects_en.pdf.

European Commission (2021), 'Guidance note - Potential misuse of research', https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf.

European Commission (2021). 'Guidance note - Research with exclusive focus on civil applications', https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-research-focusing-exclusively-on-civil-applications_he_en.pdf.

European Commission (2021), *Study on the effectiveness of public innovation support for SMEs in Europe – Final report*, DG Internal Market, Industry, Entrepreneurship and SMEs, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2826/7745.

European Commission (2021), 'The Defence Transfers Directive: Handbook for SMEs', https://defence-industry-space.ec.europa.eu/document/download/f0be94c6-223d-4910-8f8b-bba778a8b07a_en?filename=The%20Defence%20Transfers%20Directive%20-%20Handbook%20for%20SMEs%20%28EN%29.pdf.

European Commission (2021), 'The Ethics Appraisal Scheme in Horizon Europe [presentation]', https://www.bbmri-eric.eu/wp-content/uploads/The-Ethics-Appraisal-Scheme-_BBMRI-webinar-september-2021_version-for-dessimination.pdf.

European Commission (2022), 'Tackling R&I foreign interference', Staff Working Document, DG Research and Innovation, https://op.europa.eu/en/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1/language-en.

European Commission (2023), 'EU enables coordinated export controls by compiling national lists', https://policy.trade.ec.europa.eu/news/eu-enables-coordinated-export-controls-compiling-national-lists-2023-10-26_en.

European Commission (2024), *Align, Act, Accelerate: Research, Technology and Innovation to boost European Competitiveness*, DG Research and Innovation, Publications Office of the European Union, Luxembourg, https://op.europa.eu/en/publication-detail/-/publication/2f9fc221-86bb-11ef-a67d-01aa75ed71a1/language-en.

European Commission (2024), 'Horizon Europe implementation, Key figures 2021-2023', DG Research and Innovation, https://op.europa.eu/en/publication-detail/-/publication/311df01e-215f-11ef-a251-01aa75ed71a1/language-en.

European Commission (2024), *Annual Report on European SMEs 2023/2024*, Joint Research Centre, DG Internal Market, Industry, Entrepreneurship and SMEs, https://single-market-economy.ec.europa.eu/smes/sme-strategy-and-sme-friendly-business-conditions/sme-performance-review_en.

European Commission (2024), *SME participation in Horizon Europe – Key figures (and key issues) in the first three years*, DG Research and Innovation, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2777/576670.

European Commission (2024), *Horizon Europe strategic plan 2025-2027*, DG Research and Innovation, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2777/092911.

European Commission (2024), *Horizon IP scan – Helping SMEs manage and valorise intellectual property in R&I collaborations*, European Innovation Council and SMEs Executive Agency, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2826/778582.

European Commission (2024), 'Mission Letter for Commissioner Ekaterina Zaharieva from President Ursula von der Leyen', https://commission.europa.eu/document/download/833e082a-0c39-4bc6-a119-e0760ebc7360_en?filename=mission-letter-zaharieva.pdf.

European Commission (2025), Annex to the Commission Implementing Decision on the financing of the European Defence Fund and the adoption of the work programme for 2025 - Part 2 and amending Implementing Decisions C(2023) 2296 final and C(2024) 1702 final as regards financial support to third parties.

European Commission (2025), Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/821 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, COM(2025)19 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=celex:52025DC0019.

European Export Control Association for Research Organisations (n.d.), 'About EECARO', https://eecaro.eu/about-eecaro/.

European Export Control Association for Research Associations (n.d.), 'EECARO position papers', https://eecaro.eu/position-papers/.

European Export Control Association for Research Associations (2022), 'Comments to EU-US Trade and Technology Council' s Export Controls Working Group', https://eecaro.eu/publish/pages/6178/eecaro_ttc_input_wg7_export_controls.pdf.

European Export Control Association for Research Organisations (2024), 'Feedback on the White Paper on Export Controls', https://eecaro.eu/position-papers/.

European Export Control Association for Research Organisations (2024), 'Feedback on the White Paper on options for enhancing support for research and development involving technologies with dual-use potential', https://eecaro.eu/position-papers/.

European External Action Service (2024), '26th Annual Report on Arms Exports (for 2023) launched', https://tinyurl.com/4ra33smb.

Eurostat (2024), 'Enterprises with research and development (R&D) activities during 2018 and 2020 by NACE Rev. 2 activity and size class', https://ec.europa.eu/eurostat/databrowser/product/page/INN_CIS12_INRD.

Eurostat (2025), 'International trade in goods by enterprise size', https://ec.europa.eu/eurostat/statistics-explained/index.php?title=International_trade_in_goods_by_enterprise_size#Highlights.

Finnish Ministry for Foreign Affairs (2024), Export control of dual-use items: Obligations for companies, https://um.fi/documents/35732/0/Export+control+of+dual-use+items_2024_engl.pdf/8d57bffc-9b27-08a9-2d0c-32cf0ea3042e?t=1733233051212.

Fiott, D. (2019), 'The Valley of Death: Managing risk and resources'. In Fiott, D. (ed.), *Strategic Investment: Making geopolitical sense of the EU's defence industrial policy*, European Union Institute for Security Studies, 30-40, http://www.jstor.org/stable/resrep21145.7.

Japanese Ministry of Ecconomy, Trade and Industry (2025), Security Export Guidance, https://www.meti.go.jp/policy/anpo/seminer/shiryo/guidance_english.pdf.

Masson, H., (2024), 'European Defence Fund: Beneficiary profile after two calls for proposals (2021-2022)', Foundation for Strategic Research, https://www.frstrategie.org/sites/default/files/documents/specifique/2023/EDF2022-2021-STATS.pdf.

Ministerial Conference on the European Research Area (2020), *Bonn Declaration on Freedom of Scientific Research*, https://mbu.cas.cz/wp-content/uploads/2024/07/57eb65a9-8166-48f9-8a31-c8c4aef6cd3c.pdf.

Norwegian Directorate for Higher Education and Skills (2025), 'Export control of knowledge transfer and international sanctions', https://hkdir.no/en/guidelines-and-tools-for-responsible-international-knowledge-cooperation/international-research-and-innovation-cooperation/export-control-of-knowledge-transfer-and-international-sanctions.

Ramahandry, T., Bonneau, V., Bani, E., Vlasov, N., Flickenschild, M. et al. (2021), *Key enabling technologies for Europe's technological sovereignty*, European Parliament, Panel for the Future of Science and Technology.

Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013, https://eur-lex.europa.eu/eli/reg/2021/695/oj/eng.

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, https://eur-lex.europa.eu/eli/reg/2021/821/oj/eng.

Research Foundation Flanders (n.d.), 'Research security', https://www.fwo.be/en/about-fwo/research-policy/research-security.

Research Foundation Flanders (2017), 'General Regulations: Article 4ter - Research security', https://www.fwo.be/en/support-programmes/regulations/general-regulations.

Research Foundation Flanders (2025), 'Research Security Appraisal [presentation]', https://fwo.be/media/y50jssyu/presentation-implementation-of-fwo-s-research-security-policy-in-online-application-forms.pdf.

Sánchez Cobaleda, A. (2020), 'Definitions of concepts: Dual-use goods'. In A Decade of Evolution of Dual-Use Trade Control Concepts: Strengthening or Weakening Non-Proliferation of WMD, University of Liège, European Studies Unit.

Sirtori, E., Banfi, S., Canzian, G., Giffoni, F., Boschmans, K., et al. (2024), *SMEs and Open Strategic Autonomy*, DG Internal market, Industry, Entrepreneurship and SMEs, Publications Office of the European Union, Luxembourg, https://op.europa.eu/en/publication-detail/-/publication/4fe14ca4-3e6c-11ef-ab8f-01aa75ed71a1/language-en.

UK Government (2021), 'Export controls applying to academic research', Guidance.

UK Government (2021), 'Exporting military or dual-use technology : definitions and scope', Guidance.

Vandresse, B., Costa Cardoso, J., Attorri, R., and Atangana Mvogo, W. (2023), *European startup scoreboard – Feasibility study*, DG Research and Innovation, Publications Office of the European Union, Luxembourg, https://data.europa.eu/doi/10.2777/254834.

Policy strategies supporting dual-use research and innovation – international examples and benchmarks

Aharonov, A. C., and Lax, Y. (2024), 'חוקי השבבים של ארצות הברית ושל האיחוד האירופי (U.S. and EU Chip Laws)', https://fs.knesset.gov.il/25/Committees/25_cs_bg_4564188.pdf.

Air Force Research Laboratory (n.d.), 'AFWERX – Accelerating Agile Innovation for the U.S. Air Force', https://afwerx.com/.

Alvarez-Aragones, P. (2024), 'The New Arms Race in Dual-Use Technologies', IE Insights, https://www.ie.edu/insights/articles/the-new-arms-race-in-dual-use-technologies/.

Angelier, C. (2024), 'La Recherche Publique, Une Assurance Santé Pour Les Entreprises. Posologie: Abusez Des Cifre!', La Lettre de l'ANRT, https://la-lettre.anrt.asso.fr/lettre/Ymk.

Arcesati, A., Ghiretti, F., and Schwaag Serger, S. (2023), 'In Research Collaboration, Drawing Red Lines with China Isn't Easy', Merics, https://merics.org/en/comment/research-collaboration-drawing-red-lines-china-isnt-easy.

Atkinson, R. D. (2024), 'China Is Rapidly Becoming a Leading Innovator in Advanced Industries'. Information Technology and Innovation Foundation, https://itif.org/publications/2024/09/16/china-is-rapidly-becoming-a-leading-innovator-in-advanced-industries/.

Australian Government (2021), 'Guidelines to Counter Foreign Interference in the Australian University Sector', https://www.education.gov.au/download/4798/guidelines-counter-foreign-interference-australian-university-sector/24603/guidelines-counter-foreign-interference-australian-university-sector/pdf.

Axis Communications (n.d.), 'Axis Communications', https://www.axis.com/sv-se.

Baldwin, H. (2024), *Critical Dual-Use Technologies: Commercial, Regulatory, Societal and National Security Challenges*, NATO Parliamentary Assembly, https://www.nato-pa.int/document/2024-dual-use-technologies-report-baldwin-051-esc.

Barker, T., and Hagebölling, D. (2022), 'A German Digital Grand Strategy: Integrating Digital Technology, Economic Competitiveness, and National Security in Times of Geopolitical Change', German Council on Foreign Relations (DGAP), https://dgap.org/en/research/publications/german-digital-grand-strategy.

Barker, T., and Hagebölling, D. (2022), 'Deutschlands wirtschaftliche Sicherheit und Technologie', Deutsche Gesellschaft für Auswärtige Politik, https://dgap.org/system/files/article_pdfs/DGAP-Report-2022-DE-Kapitel_05_0.pdf.

Blagoeva, D., Pavel, C., Wittman, D., Huisman, J., Pasimeni, F. (2019), *Materials dependencies for dual-use technologies relevant to Europe's defence sector*, Joint Research Centre, Publications Office of the European Union, Luxembourg, https://op.europa.eu/en/publication-detail/-/publication/7799d4a7-56b9-11ea-aece-01aa75ed71a1/language-en.

Blasi, B. (2024), *Horizon Europe: Protecting academic freedom – Strengthening and improving implementation of Recital 72*, European Parliament Research Service, https://op.europa.eu/en/publication-detail/-/publication/17ebc05b-32aa-11ef-a61b-01aa75ed71a1/language-en.

British Business Bank (n.d.), 'National Security Strategic Investment Fund', https://www.british-business-bank.co.uk/for-financial-advisors/equity-finance/national-security-strategic-investment-fund.

British Business Bank (n.d.), 'About NSSIF', https://www.british-business-bank.co.uk/for-financial-advisors/equity-finance/national-security-strategic-investment-fund/about-us.

British Council, and Universities UK International (2024), 'Managing Risk and Developing Responsible Transnational Education (TNE) Partnerships', https://www.britishcouncil.org/sites/default/files/managing_risk_and_developing_responsible_transnational_education_partnerships.pdf.

Burwell, F. (2024), 'Looking ahead to the next chapter of US-EU digital collaboration', Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/report/looking-ahead-to-the-next-chapter-of-us-eu-digital-collaboration/.

Business Finland (n.d.), 'Defense and Digital Resilience: New Global Competitive Edge from Comprehensive Digital Security and Defense', https://www.businessfinland.fi/en/for-finnish-customers/services/programs/defense-digital-resilience.

European Commission (n.d.), 'EUDIS', https://eudis.europa.eu/index_en.

CESAER (2023), 'Keeping science open? Current challenges in the day-to-day reality of universities - White paper', https://www.cesaer.org/content/5-operations/2023/202310-white-paper-keeping-science-open/20231018-white-paper-keeping-science-open.pdf.

CESAER (2023), 'Workshop on Research Security – GSF-01 Multilateral Dialogue on Principles and Values in International Research & Innovation Cooperation', https://www.cesaer.org/content/3-task-forces/2022-2023/task-force-openness-science-technology/20231207-research-security-event.pdf.

CESAER (2024), 'Strengthen Dual-Use Technologies by Enhancing EU Defence Funding', https://doi.org/10.5281/ZENODO.11091518.

Charatsis, C. (2017), 'Dual-Use Research and Trade Controls: Opportunities and Controversies', *Strategic Trade Review Volume*, 3(4), https://strategictraderesearch.org/wp-content/uploads/2017/09/Dual-use-Research-and-Trade-Controls-Opportunities-and-Controversies-1.pdf.

Chmielewski, M. (2022), 'TECHNOLOGIE PRZEŁOMOWE W BUDOWIE ODPORNOŚCI PAŃSTWA', https://doi.org/10.13140/RG.2.2.26178.86729.

Colecchia, A. (2025), 'OECD STI Outlook 2025 (Work in Progress): International Cooperation and Competition in Science and Technology and the Geopolitical Context', OECD Committee for Scientific and Technological Policy, https://www.jst.go.jp/crds/sympo/20250122/pdf/20250122_presentation02.pdf.

Commission Recommendation (EU) 2021/1700 of 15 September 2021 on internal compliance programmes for controls of research involving dual-use items under Regulation (EU) 2021/821 of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, https://eur-lex.europa.eu/eli/reco/2021/1700/oj/eng.

Cueto, J. (2024), 'Five Eyes International Intelligence Alliance Launches Collaborative Security Initiative'. Lexpert Business of Law, https://www.lexpert.ca/news/features/five-eyes-international-intelligence-alliance-launches-collaborative-security-initiative/389591.

DAAD KIWi (n.d.), 'KIWi at a Glance', https://static.daad.de/media/daad_de/pdfs_nicht_barrierefrei/infos-services-fuer-hochschulen/kompetenzzentrum/dokumente/kiwi_at_a_glance.pdf.

Defence and Security Accelerator (2024), 'Defence and Security Accelerator - Strategy 2024-26', https://assets.publishing.service.gov.uk/media/679212d29f5b6adc1581ea0d/DASA_Strategy_2024-26.pdf.

Defence Industry Europe (2025), 'Sweden Procures VIKING Uncrewed Ground Vehicle for Autonomous Military Programme', https://defence-industry.eu/sweden-procures-viking-uncrewed-ground-vehicle-for-autonomous-military-programme/.

Defence Innovation Unit (n.d.), 'Who are we/Our mission', https://www.diu.mil/about.

Defense Acquisition Program Administration (n.d.), 'Defense Acquisition Program Administration', https://www.dapa.go.kr/dapa_en/main.do.

Defense Advanced Research Projects Agency (n.d.), 'About DARPA', https://www.darpa.mil/about.

Dell'Aquila, M., Kunze, L., Renda, A., Reynolds, N., Vu, H., and Yeung T. (2025), 'Towards an Ambitious FP10 – Shaping Europe's Role In The World Through Research And Innovation', Centre for European Policy Studies, https://cdn.ceps.eu/wp-content/uploads/2025/01/6g05pHvX-Towards-an-ambitious-FP10-with-cover.pdf.

Deloitte Corporate Finance Israel (2024), 'Israel Cyber Industry Overview', https://www2.deloitte.com/content/dam/Deloitte/il/Documents/risk/Israel-Cyber-Industry-Overview-02.pdf.

Deutscher Bundestag (2024), 'Pläne der Bundesregierung zur Forschungssicherheit im Lichte der Zeitenwende', Parliamentary analysis, https://dserver.bundestag.de/btd/20/127/2012720.pdf.

Devaux, J. P., and Schnitzler, G. (2020), 'Defence Innovation: New Models and Procurement Implications. The French Case', Armament Industry European Research Group, https://www.iris-france.org/149701-defence-innovation-new-models-and-procurement-implications-the-french-case/.

Draghi, M. (2024), *The future of European competitiveness: A competitiveness strategy for Europe*, https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en.

Duszczyk, M. (2025), 'Rodzimy sektor bezpieczeństwa potrzebuje polskich innowacji (The domestic security sector needs Polish innovations)', Rzeczpospolita, https://www.rp.pl/orzel-innowacji/art41746211-rodzimy-sektor-bezpieczenstwa-potrzebuje-polskich-innowacji.

European Commission (n.d.), 'Strategic Autonomy and European Economic and Research Security', https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/strategic-autonomy-and-european-economic-and-research-security_en.

European Commission (2022), 'Tackling R&I foreign interference', Staff Working Document, DG Research and Innovation, https://op.europa.eu/en/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1/language-en.

European Commission (2023), *Joint Communication on European Economic Security Strategy*, JOIN/2023/20 final, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52023JC0020.

European Commission (2024), *Proposal for a Council Recommendation on enhancing research security*, COM(2024) 26 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2024:26:FIN.

European Commission (2024), *White Paper on options for enhancing support for research and development involving technologies with dual-use potential*, COM(2024)27 final, https://op.europa.eu/en/publication-detail/-/publication/1a54ebcd-bb98-11ee-b164-01aa75ed71a1/language-en.

European Commission (2024), European Chips Act, https://digital-strategy.ec.europa.eu/en/policies/european-chips-act.

European Commission (2025), 'European Defence Fund: Over €1 Billion to Drive Next-Generation Defence Technologies and Innovation', DG Defence Industry and Space, https://defence-industry-space.ec.europa.eu/european-defence-fund-over-eu1-billion-drive-next-generation-defence-technologies-and-innovation-2025-01-30_en.

Farrow, A. E. (2023), 'Modernization and the Military-Civil Fusion Strategy', Air University (AU), https://www.airuniversity.af.edu/JIPA/Display/Article/3533572/modernization-and-the-military-civil-fusion-strategy/.

Federal Ministry of Education and Research (2024), 'Position Paper of the German Federal Ministry of Education and Research on Research Security in Light of the Zeitenwende'.

Fincantieri (n.d.), 'Funded projects', https://www.fincantieri.com/en/innovation/innovation-projects/.

FLIR (2022), 'Teledyne FLIR Helps to Keep Airspace Surrounding Swedish Critical Infrastructure Free of Drones', The Engineer, https://www.theengineer.co.uk/content/product/teledyne-flir-helps-to-keep-airspace-surrounding-swedish-critical-infrastructure-free-of-drones/.

Frantzman, S. J. (2023), 'How Israel's military is prioritizing dual-use start-ups to accelerate defense tech', Breaking Defense, https://breakingdefense.com/2023/07/how-israels-military-is-prioritizing-dual-use-start-ups-to-accelerate-defense-tech/.

Frantzman, S. J. (2024), 'Israel's Ministry of Defense quintupled start-up funding in last year', Breaking Defense, https://breakingdefense.com/2024/12/israels-ministry-of-defense-pours-money-into-start-ups/.

Gallo, M. E. (2025), 'The Defense Innovation Ecosystem', Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF12869.

Getz, D., Shacham, O. K., Klein, R., Tzena, R., Rosenberg, S., et al. (2018), 'בינה מלאכותית, מדעי הנתונים ורובוטיקה "חכמה – דו"ח ראשון" (Artificial Intelligence, Data Science, and Smart Robotics – First Report)', מכון נאמן למדיניות לאומית (Samuel Neaman Institute for National Policy Research).

González, R. J. (2024), 'How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex'. Watson Institute for International & Public Affairs, https://watson.brown.edu/costsofwar/files/cow/imce/papers/2023/2024/Silicon%20Valley%20MIC.pdf.

Government Offices of Sweden (2024), *Strategic Direction for Defence Innovation*, Ministry of Defence, https://www.government.se/information-material/2024/05/strategic-direction-for-defence-innovation/.

Government of Japan (2024), 'Strengthening Collaboration Between Japan and the Republic of Korea in Advanced Science and Technology', Kizuna, https://www.japan.go.jp/kizuna/2024/02/collaboration_between_japan_and_the_rok.html.

Greenacre, M., and Matthews, D. (2024), 'EU Commission Launches Bid to Expand Funding of Dual-Use Research in Horizon Europe's Successor', Science|Business, https://sciencebusiness.net/news/dual-use/eu-commission-launches-bid-expand-funding-dual-use-research-horizon-europes-successor.

Greenberg, T. (2025), 'Israel creates hub to hasten military AI, autonomy research', Defence News, https://www.defensenews.com/global/mideast-africa/2025/01/02/israel-creates-hub-to-hasten-military-ai-autonomy-research/.

Haanpää, H., Heurlin, J., Heikkinen, K., Huimala, M., and Kuha, R. (2025), 'Expansion of the Finnish FDI Screening Regime Expected'. Hannes Snellman, https://www.hannessnellman.com/news-and-views/blog/expansion-of-the-finnish-fdi-screening-regime-expected/.

Henry, D. (2024), 'US, Japan to Conduct Research Exchanges on Emerging Tech', Department of Homeland Security, https://executivegov.com/2024/11/us-japan-science-technology-collaboration/.

Hudson, R. L. (2024), 'How Will the New US Research Security Centre Work?', Science|Business, https://sciencebusiness.net/news/r-d-funding/how-will-new-us-research-security-centre-work.

Innovation, Science and Economic Development Canada (2023), 'National Security Guidelines for Research Partnerships', https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships.

IQT (n.d.), 'Homepage', https://www.iqt.org/.

Israel Innovation Authority (2024), 'A Year Since October 7: A Situation Report on the Israeli High-Tech Sector', https://israeltrade.org.au/2024/09/26/a-year-since-october-7-a-situation-report-on-the-israeli-high-tech-sector/.

Israel Ministry of Defence (n.d.), 'DECA: Defense Export Control Agency', https://english.mod.gov.il/About/Defense_Exports/Pages/DECA_Defense_Export_Control_Agency.aspx.

Israel Ministry of Defence (n.d.), 'Military Research and Development', https://english.mod.gov.il/About/Innovative_Strength/Pages/Military_Research_and_Development.aspx.

Italian Space Industry (n.d.), 'Italian Aerospace Clusters', https://italianspaceindustry.it/italian-aerospace-clusters/.

Järvinen, S. O. (2024), 'Cautious Data-Driven Evolution: Defence AI in Finland'. In Borchert, H., Schütz, T., and Verbovszky, J. (eds.), *The Very Long Game: 25 Case Studies on the Global State of Defense AI*, Cham: Springer Nature Switzerland, 127-148. https://doi.org/10.1007/978-3-031-58649-1_6.

JASON advisory group (2024), *Safeguarding the Research Enterprise*, U.S. National Science Foundation, https://www.nsf.gov/news/nsf-announcement-jason-report-safeguarding.

Joshi, M. (2022), 'China's Military-Civil Fusion Strategy, the US Response, and Implications for India', Observer Research Foundation, https://www.orfonline.org/research/china-s-military-civil-fusion-strategy-the-us-response-and-implications-for-india.

KARVE (2023), 'UK Defence Innovation Funds & Accelerator Programmes', https://www.karveinternational.com/insights/uk-defence-innovation-funds-accelerator-programmes.

Kauppila, L., and Cappelin, B. (2023), 'The China Dilemma in Foreign Direct Investment Screening: Comparing the Finnish and Swedish Approaches', Swedish National China Centre, https://kinacentrum.se/en/publications/the-china-dilemma-in-foreign-direct-investment-screening-comparing-the-finnish-and-swedish-approaches/.

Kelly, B., and Qian, J. (2025), 'U.S. and China Just Set New Road Rules for Science Collaboration. Americans Will Benefit If We Don't Scrap Joint Research', ChinaFile, https://www.chinafile.com/reporting-opinion/viewpoint/us-and-china-just-set-new-road-rules-science-collaboration-americans.

Kolliarakis, G. (2022), 'Anticipatory Governance of Emerging and Disruptive Technologies with Dual-Use Potential', DGAP - German Council on Foreign Relation, https://dgap.org/en/research/publications/anticipatory-governance-emerging-and-disruptive-technologies-dual-use.

Korea Industry Daily (2023). '반도체·방산기술 해외 유출시 최대 징역 15년 [Up to 15 Years Imprisonment for Overseas Leakage of Semiconductor and Defense Technology]'. 정보통신신문, http://www.koit.co.kr/news/articleView.html?idxno=92813.

Kousuke S. (2024), 'Japan's Push for a Dual-Use Defence Startup Ecosystem', East Asia Forum, https://eastasiaforum.org/2024/12/26/japans-push-for-a-dual-use-defence-startup-ecosystem/.

Kruczkowska, E. (2024), 'Inwestycje dual-use: nowy trend czy rzeczywista potrzeba?', startup.pfr.pl, https://startup.pfr.pl/artykul/inwestycje-dual-use-nowy-trend-czy-rzeczywista-potrzeba.

Kruppa, M., and Perry, A. (2024), 'Silicon Valley's Hot Talent Pipeline Is an Israeli Army Unit', The Wall Street Journal, https://www.wsj.com/tech/silicon-valleys-hot-talent-pipeline-is-an-israeli-army-unit-e8368b4d.

Laje, D. (2024), 'Small Businesses Adapt for Advantage in Dual-Use Era', AFCEA, https://www.afcea.org/signal-media/technology/small-businesses-adapt-advantage-dual-use-era.

Lawrence, C. (2024), 'Polish startups set to benefit from new €100M Defence Fund', Tech.eu, https://tech.eu/2024/12/02/poland-takes-a-step-towards-eur100m-defence-fund-a-step-towards-technological-sovereignty/.

Leonardo (n.d.), 'Collaborative Research Projects', https://www.leonardo.com/en/innovation-technology/funded-research-projects.

Linney, B., Cook, R., and Jansen, S. (2025), 'CFIUS Has Circled Its Civil Enforcement Wagons — Trump 2.0 Is Likely to Build upon Activities Begun by Biden Administration', Reuters, https://www.reuters.com/legal/legalindustry/cfius-has-circled-its-civil-enforcement-wagons-trump-20-is-likely-build-upon-2025-02-13/.

Longfield, L. (2024), *The Security of Research Partnerships Between Canadian Universities, Research Institutions and Entities Connected to the People's Republic of China*, House of Commons of Canada, https://publications.gc.ca/collections/collection_2024/parl/xc79-1/XC79-1-1-441-10-eng.pdf.

Madsen, M. (2020), 'Defence Innovation Unit SBIR/STTR', https://rt.cto.mil/wp-content/uploads/2020/10/SBIR_STTR-DIU-Orientation_Sept2020.pdf.

Marcucci, M. E. (2024), 'From Lasers to Lavender: Will Israel's Dual-Use Technology Lead To Dual-Use Societies?', Turning Point, https://turningpointmag.org/2024/04/28/from-lasers-to-lavender-will-israels-dual-use-technology-lead-to-dual-use-societies/.

Marklund, G., Stenberg, L., Johansson, D., Lundin, N., and Hallding K. (2023), *Omvärldsanalys - Analysbilaga till Vinnovas Underlag till Regeringens Forsknings- Och Innovationspolitik*, Vinnova, https://www.vinnova.se/en/publikationer/analysis-appendix-to-vinnovas-basis-for-the-governments-research-and-innovation-policy-2025-2028/.

Marrone, A., and Gilli, A. (2020), 'Defence Innovation: New Models and Procurement Implications. The Italian Case', Istituto Affari Internazionali, https://www.iai.it/en/pubblicazioni/c09/defence-innovation-new-models-and-procurement-implications-italian-case.

Matthews D. (2023), 'Europe Needs to Hone Its "Technological Edge" in Areas Where It Leads, Think Tank Fellows Say', Science|Business, https://sciencebusiness.net/news/sovereignty/europe-needs-hone-its-technological-edge-areas-where-it-leads-think-tank-fellows.

Mc Nicholas, A. (2024), 'China's Military-Civil Defusion', The Wire China, https://www.thewirechina.com/2024/09/22/chinas-military-civil-defusion/.

Ministère des Armées (n.d.), 'Agence de l'Innovation de Défense', https://www.defense.gouv.fr/aid.

Ministerstwo Obrony Narodowej (2024), 'Resortowa strategia sztucznej inteligencji do roku 2039', https://www.gov.pl/web/obrona-narodowa/resortowa-strategia-sztucznej-inteligencji-do-roku-2039.

Ministry of Defence of Finland (2024), 'Government Defence Report', http://urn.fi/URN:ISBN:978-951-663-471-8.

Ministry of Defence of Japan (2019), 'Defense of Japan 2019 – Section 4-2-2: Initiatives in the Space Domain', https://www.mod.go.jp/en/publ/w_paper/wp2019/pdf/DOJ2019_4-2-2.pdf.

Mundell, I. (2022), 'The Ecosystem: In Europe, Defence Innovation Is the New Black', Science|Business, https://sciencebusiness.net/news/ecosystem-europe-defence-innovation-new-black.

Munro, B. (2024), 'Tech Industry Is the New Defence Industrial Base', The Strategist, https://www.aspistrategist.org.au/tech-industry-is-the-new-defence-industrial-base/.

National Defence Training Association of Finland (n.d.). 'What Is the MPK?', https://mpk.fi/en/.

National Protective Security Authority (2024), 'Trusted Research Guidance for Academics', https://www.npsa.gov.uk/system/files/trusted-research-guidance-for-academia-digital-july24.pdf.

National Protective Security Authority (2024), 'Trusted Research Guidance for Senior Leaders', https://www.npsa.gov.uk/system/files/npsa-trusted-research-guidance-for-senior-leaders_0_1_0.pdf.

NATO (n.d.), 'Defence Innovation Accelerator for the North Atlantic', https://www.diana.nato.int/.

Niinistö, S. (2024), Safer Together – Strengthening Europe's civilian and military preparedness and readiness, https://commission.europa.eu/document/5bb2881f-9e29-42f2-8b77-8739b19d047c_en.

O'Dwyer, G. (2024), 'Finland to Host NATO Tech Centers, Revamp Cybersecurity Strategy', C4ISRNet, https://www.c4isrnet.com/cyber/2024/03/26/finland-to-host-nato-tech-centers-revamp-cybersecurity-strategy/.

OECD (2023), 'OECD Science, Technology and Innovation Outlook 2023: Enabling Transitions in Times of Disruption', https://doi.org/10.1787/0b55736e-en.

Osawa, J. (2023), 'How Japan Defines Economic Security', Wilson Center, https://www.wilsoncenter.org/publication/how-japan-defines-economic-security.

Pannier, A. (2023), 'Balancing Security and Openness for Critical Technologies: Challenges for French and European Research', Institut français des relations internationales, https://www.ifri.org/en/studies/balancing-security-and-openness-critical-technologies-challenges-french-and-european.

Pellerin, C. (2016), 'Deputy Secretary: Third Offset Strategy Bolsters America's Military Deterrence', U. S. Department of Defense, https://www.defense.gov/News/News-Stories/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/.

Polski Fundusz Rozwoju (n.d.), 'Rozwój technologii podwójnego zastosowania wspiera polską gospodarkę i bezpieczeństwo', https://pfr.pl/artykul/rozwoj-technologii-podwojnego-zastosowania-wspiera-polska-gospodarke-i-bezpieczenstwo.

Porter, A. (2023), 'DFARS Compliance for DoD Contractors: Best Practices'. BigID, https://bigid.com/blog/dfars-compliance-best-practices/.

Prime Minister's Office of Finland (2024), *Finland's Cyber Security Strategy 2024–2035*, https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165893/VNK_2024_13.pdf.

PwC (2022), 'The CHIPS Act: What It Means for the Semiconductor Ecosystem', https://www.pwc.com/us/en/library/chips-act.html.

Ramage, T. (2024) 'Timeline of the South Korean Government's AI Efforts', Korea Economic Institute of America (KEI), https://keia.org/the-peninsula/timeline-of-the-south-korean-governments-ai-efforts/.

Rat für technologische Souveränität (2024), 'Schlüsseltechnologien im Fokus – Der Wettlauf um industrie- und technologiepolitische Führung: „Technologische Souveränität" im internationalen Vergleich'.

Raubo, J. M. (2024), 'Technologie podwójnego przeznaczenia wyzwaniem dla odporności kraju [OPINIA]', https://defence24.pl/przemysl/technologie-podwojnego-przeznaczenia-wyzwaniem-dla-odpornosci-kraju-opinia.

Rausch J. (2021), 'Commercialized Militarization: China's Military-Civil Fusion Strategy', The National Bureau of Asian Research, https://www.nbr.org/publication/commercialized-militarization-chinas-military-civil-fusion-strategy/.

Regeringskansliet (2024), 'Excellent forskning och innovationskraft premieras i den största forsknings- och innovationspropositionen någonsin', https://www.regeringen.se/pressmeddelanden/2024/12/excellent-forskning-och-innovationskraft-premieras-i-den-storsta-forsknings--och-innovationspropositionen-nagonsin/.

Research and Innovation Security and Competitiveness Institute (n.d.), 'Programs and Partners', Texas A&M University System, https://risc.tamus.edu/.

Research Compliance Office (n.d.), 'Research Security - FAQ for International Affiliations Foreign Engagements', Berkeley Labs, https://rco.lbl.gov/research-security/faq-for-international-affiliations-foreign-engagements/.

Reuters (2024), 'Poland Investigating Russian Espionage, Security Agency Says', https://www.reuters.com/world/europe/poland-investigating-russian-espionage-security-agency-says-2024-03-28/?utm_source=chatgpt.com.

Ruitenberg, R. (2024), 'France Preps Europe's Fastest Classified Supercomputer for Defense AI', Defense News, https://www.defensenews.com/global/europe/2024/06/18/france-preps-europes-fastest-classified-supercomputer-for-defense-ai/.

Säkerhetspolisen (2024), *Säkerhetspolisen 2024-2025*, https://sakerhetspolisen.se/download/18.328c5ae9195250d81d04ad/1741953348924/L%C3%A4gesbild%202024-2025.pdf.

Schlueter, M., Giesener, M., Mayer, L., Key, L., and Hassan, M. (2025), 'Overcoming the Six Unspoken Barriers That Impede Defense Innovation', Boston Consulting Group and the Munich Security Conference, https://web-assets.bcg.com/c0/ad/ed8e25f5483aa1f42a614c0224bf/overcoming-the-six-unspoken-barriers-that-impede-defense-innovation-msc.pdf.

Schuch, K., Puukka, J., Shih, T., and Pamment, J. (2024), 'Final Report of the Mutual Learning Exercise on Tackling Foreign Interference in Research and Innovation (R&I)', Horizon Europe Policy Support Facility.

Schwägerl, C. (2024), 'Vom Weltgeist Zum Machthebel', *Internationale Politik*, 1(1), 71-75.

Science and Technology Policy Institute (2024). '국방 혁신과 듀얼유즈 전략: 산업계 참여 확대를 위한 정책방향 [Defense Innovation and the Dual-Use Strategy: Industrial Participation and Policy Recommendations]', https://www.stepi.re.kr/site/iiccko/ex/bbs/View.do;jsessionid=4F4A0404F631E14A25B4D936714B7D6F?cbIdx=1334&bcIdx=40869.

Shih, T. (2023), 'Responsible Internationalization - Why, What, and How?', Lund: Open Science Framework, https://doi.org/10.31219/osf.io/gz5m8.

Shroff, A. (2020), '"Made in China 2025" Disappears in Name Only'. Indo-Pacific Defense Forum, https://ipdefenseforum.com/2020/03/made-in-china-2025-disappears-in-name-only/.

Silverberg, E., Sharpe, J., and Murray, R. (2025), 'Making AUKUS work: The case for an Indo-Pacific defense innovation consortium', Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/making-aukus-work-the-case-for-an-indo-pacific-defense-innovation-consortium/.

SMART (n.d.), 'Scholarship-for-Service Program', https://www.smartscholarship.org/smart.

SPD-Bundestagsfraktion (2024), 'Stärkung Der Sicherheits- Und Verteidigungsindustrie in Deutschland Und Europa'. https://www.spdfraktion.de/system/files/documents/position-staerkung-sicherheits_und-verteidigungspolitik.pdf.

Starburst (2023), 'The Rise in Dual-Use Technologies: A Paradigm Shift', https://starburst.aero/news/the-rise-in-dual-use-technologies/.

Steve Blank (n.d.), 'Steve Blank Secret History', https://steveblank.com/secret-history/.

Strander, Y., Marklund, G., Zika-Viktorsson, A., Stenberg, L., Lundin, N. et al. (2023), 'Acceleration mot en hållbar framtid - Vinnovas inspel till regeringens forsknings- och innovationsproposition', Vinnova, https://www.regeringen.se/contentassets/5eee3b9b4a32457ea9a5fae3cf2e0bbc/vinnova.pdf.

Strouse, G. F., Saundry, C. M., Wood, T., Bennett, P. A., and Bedner, M. (2023), *Safeguarding International Science : Research Security Framework*, National Institute of Standards and Technology, https://doi.org/10.6028/NIST.IR.8484.

Sutter, K. M., and Sutherland, M. D. (2021), 'China's 14th Five-Year Plan: A First Look', Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF11684.

Swedish Council for Higher Education, Swedish Research Council, and Vinnova (2024), *Responsible Internationalisation – Interim Report on a Government Assignment 2024*, https://www.uhr.se/globalassets/_uhr.se/publikationer/2024/responsible-internationalisation---interim-report-on-a-government-assignment-2024.pdf.

Swedish Council for Higher Education, Swedish Research Council, and Vinnova (2024), *National Support Function for Responsible Internationalisation – Final Report 2025*, https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf.

SwissCore (2024), 'Commission Adopts Economic Security Package', https://www.swisscore.org/commission-adopts-economic-security-package/.

TechUK (2025), 'Ministry of Defence Announces New Support for SMEs', https://www.techuk.org/resource/ministry-of-defence-announces-new-support-for-smes.html.

Teknikföretagen, and SOFF (2023), 'En nationell teknologi- och innovationsstrategi som främjar dual use', https://soff.se/app/uploads/2023/05/En-strategi-som-framjar-dual-use.pdf.

The League of European Research Universities (2023), 'Managing and Governing Risks in International University Collaboration', https://www.leru.org/news/managing-and-governing-risks-in-international-university-collaboration.

The U.S. Senate Committee on Foreign Relations (2024), *One Step Forward, Two Steps Back: A Review of U.S.-Europe Cooperation on China*, https://www.foreign.senate.gov/imo/media/doc/risch_july_2024_one_step_forward_two_steps_back_a_review_of_useuropecooperationonchina.pdf.

TheMarker (2024), 'ישראל משנה גישה: טכנולוגיה אזרחית תחת פיקוח בטחוני' [Israel Shifts Approach: Civilian Tech Under Security Oversight]', https://www.themarker.com/labels/israelsecurity/2024-07-01/ty-article-labels/00000190-547f-ddd9-a1f1-d6ff426d0000.

Turp-Balazs, C. (2025), 'The Brain Drain Challenge: Strategies to Retain Talent in Emerging Europe', Emerging Europe, https://emerging-europe.com/analysis/the-brain-drain-challenge-strategies-to-retain-talent-in-emerging-europe/.

UK Government (2013), 'Academic Technology Approval Scheme (ATAS)', Guidance, https://www.gov.uk/guidance/academic-technology-approval-scheme.

UK Government (2015), *National Security Strategy and Strategic Defence and Security Review 2015*, https://www.gov.uk/government/publications/national-security-strategy-and-strategic-defence-and-security-review-2015.

UK Government (2023), *The UK's International Technology Strategy*, https://www.gov.uk/government/publications/uk-international-technology-strategy/the-uks-international-technology-strategy.

UK Government (2024), 'National Security and Investment Act: guidance for the higher education and research-intensive sectors', Guidance, https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors.

UK Government (2024), 'NATO DIANA UK accelerator: Welcome to the UK accelerator', Guidance, https://www.gov.uk/guidance/nato-diana-uk-accelerator-welcome-to-the-uk-accelerator.

U.S. Department of Commerce (2024), 'ICYMI: Secretary Raimondo Delivers Update on CHIPS and Science Act Implementation, Lays Road Ahead for Supercharging Innovation and Revitalizing American Semiconductor Manufacturing', https://www.commerce.gov/news/press-releases/2024/02/icymi-secretary-raimondo-delivers-update-chips-and-science-act.

U.S. Department of Commerce (2024), 'U.S. and UK Announce Partnership on Science of AI Safety', https://www.commerce.gov/news/press-releases/2024/04/us-and-uk-announce-partnership-science-ai-safety.

U. S. Department of Defense (n.d.), 'Office of Strategic Capital', https://www.cto.mil/osc/.

U.S. Department of State (2020), 'The Chinese Communist Party's Military-Civil Fusion Policy', https://2017-2021.state.gov/military-civil-fusion/.

U.S. National Science Foundation (n.d.), 'Research Security at the National Science Foundation', https://www.nsf.gov/research-security.

U.S. National Science Foundation (2024), 'Trusted Research Using Safeguards and Transparency (TRUST)', https://nsf-gov-resources.nsf.gov/files/NSF%20OCRSSP%20TRUST%20Policy%20Memo.pdf.

U.S. National Science Foundation (2024), 'NSF-Backed SECURE Center Will Support Research Security, International Collaboration' https://new.nsf.gov/news/nsf-backed-secure-center-will-support-research.

U15 Canada (2023), 'Safeguarding Research in Canada: A Guide for University Policies and Practices', https://u15.ca/wp-content/uploads/2023/06/2023-06-22.-U15-Leading-Practices-Safeguarding-Research-FINAL-3.pdf.

Van Hollen's office in the US Senate (2022), 'CHIPS and Science Act of 2022 Division A Summary - CHIPS and ORAN Investment', https://www.vanhollen.senate.gov/download/chips-and-science-act-of-2022-summary.

VTT (n.d.), 'Cybersecurity', https://www.vttresearch.com/en/ourservices/cybersecurity.

Wassenaar Arrangement Secretariat (n.d.), 'The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies', https://www.wassenaar.org/.

Wikipedia (n.d.), 'Israeli Cybersecurity Industry', https://en.wikipedia.org/w/index.php?title=Israeli_cybersecurity_industry&oldid=1256238054.

Wooyeal, P. (2024), 'South Korean Defense Industry Goes Global, and Local Too: An Econo-Tech Approach', ISPI, https://www.ispionline.it/en/publication/south-korean-defense-industry-goes-global-and-local-too-an-econo-tech-approach-169127.

XTech (n.d.), 'Small Business Igniting Big Innovation', https://xtech.army.mil/.

YL Ventures (2025), 'The State of the Cyber Nation 2024', https://www.ylventures.com/wp-content/uploads/2025/01/The-State-of-the-Cyber-Nation-2024_Full-Report_v8.pdf.

Yoon, S. (2023), 'Emerging New Military Technologies in Northeast Asia and Implications for South Korean Defense Strategy', DKI APCSS, https://dkiapcss.edu/nexus_articles/emerging-new-military-technologies-in-northeast-asia-and-implications-for-south-korean-defense-strategy/.

村山 裕三 Murayama, Yuuzou (2020), '国家安全保障と経済の両立に向けた技術戦略 (Technology Strategy for Balancing National Security and the Economy)', PHP総合研究所 (PHP Research Institute), https://thinktank.php.co.jp/wp-content/uploads/2020/10/pdf_policy_20201023.pdf.

Funding programmes for dual-use research and innovation – an international comparison

Acquisition, Technology and Logistics Agency (n.d.), 'Research & Development', https://www.mod.go.jp/atla/en/policy/research_and_development.html.

Acquisition, Technology and Logistics Agency (2024), 'Towards building a dual-use startup ecosystem', https://www.meti.go.jp/policy/mono_info_service/mono/aerospace/5_startup.pdf.

Acquisition, Technology and Logistics Agency (2025), 'ATLA Research & Development', https://www.mod.go.jp/atla/en/research/rnd_files/rnd_brochure_eng2025.pdf.

Advanced Research Projects Agency for Energy (2024), 'FY 2024 Congressional Justification', https://www.energy.gov/sites/default/files/2023-03/doe-fy-2024-budget-vol-2-arpa-e_0.pdf.

Advanced Research Projects Agency for Health (n.d.), 'Budget and Appropriations', https://arpa-h.gov/about/budget.

Allen, G. C., and Berenson, D. (2024), 'Why Is the U.S. Defense Industrial Base So Isolated from the U.S. Economy?', Center for Strategic and International Studies, https://www.csis.org/analysis/why-us-defense-industrial-base-so-isolated-us-economy.

Association of Finnish Defence and Aerospace Industries (2021), 'PIA Key Facts & Figures 2021'.

Business Finland (n.d.), 'New global competitive edge from comprehensive digital security and defence', https://www.businessfinland.fi/en/for-finnish-customers/services/programs/defense-digital-resilience.

Business Finland (2024), ‘Business Finland’s views on the main priorities in EU RDI programmes MFF 2028-2034’, https://www.businessfinland.fi/en/whats-new/news/2024/business-finlands-views-on-the-main-priorities-in-eu-rdi-programmes-mff-2028-2034.

Center for Security and Emerging Technology (2022), ‘Translation of PRC State Council (2015) Notice of the State Council on the Publication of “Made in China 2025”’, https://cset.georgetown.edu/publication/notice-of-the-state-council-on-the-publication-of-made-in-china-2025/

Congressional Research Service (2018), ‘Defense Advanced Research Projects Agency: Overview and Issues for Congress’, https://crsreports.congress.gov/product/pdf/R/R45088/10.

Congressional Research Service (2021), ‘Defense Advanced Research Projects Agency: Overview and Issues for Congress’, https://crsreports.congress.gov/product/pdf/R/R45088/15.

Congressional Research Service (2024), ‘Federal Research and Development (R&D) Funding: FY2025’, https://crsreports.congress.gov/product/pdf/R/R48307/1.

Cornell Law School (2023), ‘International Traffic in Arms Regulations (ITAR)’, Legal Information Institute, https://www.law.cornell.edu/wex/international_traffic_in_arms_regulations_(itar).

Cyranoski, D. (2017), ‘Japanese scientists call for boycott of military research’, Nature, https://doi.org/10.1038/nature.2017.21779.

Defense Advanced Research Projects Agency (n.d.), ‘Budgets and Testimony’, https://www.darpa.mil/about/budgets-testimony.

Defense Advanced Research Projects Agency (2012), ‘Doing Business With DARPA: Creating and Preventing Strategic Surprise’, https://www.acqnotes.com/Attachments/DoingBusinesswithDARPA2012.pdf.

Defense Advanced Research Projects Agency (2024), ‘Protecting Innovation: Understanding IP in DARPA Contracts’, DARPA Connect webinar, https://learning.theari.us/products/protecting-innovation-understanding-ip-in-darpa-contracts-october-30-2024.

Defense Innovation Board (2024), ‘Optimizing Innovation Cooperation with Allies and Partners’, https://innovation.defense.gov/Portals/63/20240710%20DIB%20Allies%20and%20Partners%20Study%20FINAL.pdf.

Directorate of Defense, Research and Development (n.d.), ‘INNOFENSE’, https://ddrd-mafat.mod.gov.il/en/innofense.

Directorate of Defense, Research and Development (n.d.), ‘MAFAT For Startups’, https://ddrd-mafat.mod.gov.il/en/mafat-for-startups.

Dugan, R. E., and Gabriel, K. J. (2013), ‘“Special Forces” Innovation: How DARPA Attacks Problems’, *Harvard Business Review*, 91(10), 74-84.

Frantzman, S. J. (2024), ‘Israel’s Ministry of Defense quintupled start-up funding in last year’, Breaking Defense, https://breakingdefense.com/2024/12/israels-ministry-of-defense-pours-money-into-start-ups/.

Fritz, A. (2019), ‘China’s Evolving Conception of Civil-Military Collaboration’, Center for Strategic and International Studies, https://www.csis.org/blogs/trustee-china-hand/chinas-evolving-conception-civil-military-collaboration.

Gehrke, N. (2024), ‘METI's "Towards building an ecosystem for dual-use startups" report’, Japan Startup Observer, https://japanstartupobserver.substack.com/p/metis-towards-building-an-ecosystem-b24.

Ikeda, T. (2022), ‘Japan science council says drawing line between military, civil use technology difficult’, The Mainichi, https://mainichi.jp/english/articles/20220728/p2a/00m/0na/023000c.

InnoTal (n.d.), טכנולוגיות ישראליות לצה״ל (machine translation: Israeli Technologies for the IDF), https://www.israelinnovation.org.il/innotal.

Israel Innovation Authority (n.d.), ‘Leveraging R&D for Dual Use Technologies – MEIMAD’, https://innovationisrael.org.il/en/programs/leveraging-rd-for-dual-use-technologies-meimad/.

Israel Innovation Authority (n.d.), ‘Support Program for Innovation in Selected Fields – Homeland Security (HLS)’, https://innovationisrael.org.il/en/programs/support-program-homeland-security-hls/.

Israel Innovation Authority (2020), *Israel Innovation Authority’s 2019 Innovation Report*, https://innovationisrael.org.il/en/report/innovation-report-2019/.

Israel Innovation Authority (2021), ‘Activities of the Israel Innovation Authority’s Divisions’, https://innovationisrael.org.il/en/report/activities-israel-innovation-authoritys-divisions/.

Israel Innovation Authority (2021), *2021 Annual Report: The State of High-Tech*, https://innovationisrael.org.il/sites/default/files/The%20Israel%20Innovation%20Report%202021.pdf.

Israel Innovation Authority (2022), *2022 Annual Report: The State of High-Tech*, https://innovationisrael.org.il/files-en/Annual%20Innovation%20Report%20-%20State%20of%20High-Tech%202022.pdf.

Israel Innovation Authority (2023), *2023 Annual Report: The State of High-Tech*, https://innovationisrael.org.il/en/wp-content/uploads/sites/3/2023/07/2023-The-state-of-High-Tech.pdf.

Israel Innovation Authority (2024), *2024 Annual Report: The State of High-Tech*, https://innovationisrael.org.il/wp-content/uploads/2024/06/2024-Annual-Report-The-State-of-High-Tech.pdf.

Israel Innovation Authority (2025), 'International Collaborations', https://innovationisrael.org.il/en/international-collaborations/.

Israel Innovation Authority (2025), 'International R&D and Pilot Collaborations – 2025', https://innovationisrael.org.il/en/calls_for_proposal/international-rnd-and-pilot-collaborations-2025ii/.

Israel Ministry of Defence (n.d.), 'Advancing Defense Exports', https://english.mod.gov.il/About/Defense_Exports/Pages/default.aspx.

Israel Ministry of Economy and Industry (2023), 'Export Control Agency', https://www.gov.il/en/pages/duexportcontrol-info.

Japanese Coalition Against Military Research in Academia (n.d.), 'Homepage', http://no-military-research.jp/.

Japan Ministry of Defence (n.d.), 'Research & Development', https://www.mod.go.jp/atla/en/policy/research_and_development.html.

Japan Ministry of Defence (2024), 'Press Conference by Defense Minister Kihara on Tuesday, October 1, 2024, at 11:08 AM', https://www.mod.go.jp/en/article/2024/10/e7a8d2e31c59f5f065787be9b6449b2a84565583.html.

Japan Ministry of Economy, Trade and Industry (2021), 'Security Export Control', https://www.meti.go.jp/policy/anpo/englishpage/securityexportcontrolinjapan5.pdf.

Japan Ministry of Economy, Trade and Industry (2024), 'Towards building a dual-use startup ecosystem', https://www.meti.go.jp/policy/mono_info_service/mono/aerospace/5_startup.pdf.

Japan Press Weekly (2024), 'Gov't move to promote integration between gov't, industry, and academia creates dangerous path toward becoming a war-fighting nation', https://www.japan-press.co.jp/s/news/?id=15396.

Japan Society for the Promotion of Science (2015), For the Sound Development of Science: The Attitude of a Conscientious Scientist, https://www.jsps.go.jp/english/e-kousei/ethics.html.

Korea Legislation Research Institute (2003), Foreign Trade Act, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=5000&lang=ENG.

Korea Legislation Research Institute (2018), Promotion of Technology Projects for Joint Civilian and Military Use Act, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=51447&lang=ENG.

Korea Legislation Research Institute (2020), Defense Technology Security Act, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=55217&lang=ENG.

Korea Legislation Research Institute (2023), National Research and Development Innovation Act, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=62484&lang=ENG.

Korea Legislation Research Institute (2024), Defense Acquisition Program Act, https://elaw.klri.re.kr/eng_service/lawView.do?hseq=64704&lang=ENG.

Kyodo News (2024), 'Japan to open U.S.-inspired defense tech research center in October', https://english.kyodonews.net/news/2024/08/a1295b84fbe8-japan-to-open-us-inspired-defense-tech-research-center-in-october.html.

Laje, D. (2024), 'Small Businesses Adapt for Advantage in Dual-Use Era', AFCEA, https://www.afcea.org/signal-media/technology/small-businesses-adapt-advantage-dual-use-era.

Lawrence Livermore National Laboratory (n.d.), 'By the Numbers', https://www.llnl.gov/about/by-the-numbers.

Matthews, D. (2025), 'Foreign researchers in China face tightening restrictions', Nature, https://www.nature.com/articles/d41586-025-00630-1.

Ministry for Foreign Affairs of Finland (n.d.), 'Export control', https://um.fi/export-control.

Ministry of Science and Technology of the People's Republic of China (n.d.), 'National High-tech R&D Program (863 Program)', https://en.most.gov.cn/programmes1/.

National Natural Science Foundation of China (n.d.), 'Homepage', https://www.nsfc.gov.cn/english/site_1/index.html.

National Natural Science Foundation of China (2023), 'National Natural Science Fund Guide to Programs 2023', https://www.nsfc.gov.cn/english/site_1/pdf/NationalNaturalScienceFundGuidetoPrograms2023.pdf.

NATO (n.d.), 'DIANA', https://www.diana.nato.int/.

NATO (n.d.), 'The NATO Innovation Fund', https://www.nif.fund/.

NATO (2021), *SPS Programme Annual Report 2020*, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/10/pdf/211004_NATO_SPS_AnnualReport2020.pdf.

NATO (2023), 'Science for Peace and Security Programme', https://www.nato.int/cps/en/natohq/topics_85373.htm.

NATO (2023), 'SPS Grant mechanisms', https://www.nato.int/cps/en/natohq/79910.htm.

NATO (2024), 'Countering terrorism', https://www.nato.int/cps/en/natohq/topics_77646.htm.

New Energy and Industrial Technology Development Organization (2024), 'Deep-Tech Startups Support Program (DTSU), Deep-Tech Startups Support Program in the Green Transformation field (GX)', https://www.nedo.go.jp/english/activities/activities_ZZJP_100250.html.

Nouwens, M., and Legarda, H. (2018), 'China's pursuit of advanced dual-use technologies', International Institute for Strategic Studies, https://www.iiss.org/research-paper/2018/12/emerging-technology-dominance/.

Prosser, M. J. (2023), 'Japan aims to boost defense industry with 200 startups', Indo-Pacific Defense Forum, https://ipdefenseforum.com/2023/09/japan-aims-to-boost-defense-industry-with-200-startups/.

Research Council of Finland (n.d.), 'Funding criteria and policies', https://www.aka.fi/en/about-us/decision-making-bodies/scientific-councils/scientific-council-for-natural-sciences-and-engineering/policies-of-the-research-council-for-natural-sciences-and-engineering/.

Research Council of Finland (n.d.), 'Research ethics', https://www.aka.fi/en/research-funding/responsible-science/research-ethics/.

Research Council of Finland (2024), 'Research Council of Finland to fund wide range of excellent research in 2025', Press release, https://www.aka.fi/en/about-us/whats-new/press-releases/2024/research-council-of-finland-to-fund-wide-range-of-excellent-research-in-2025/.

ROK Ministry of National Defence (2023), *National Defense Science and Technology Basic Plan (2023–2027)*, https://online.fliphtml5.com/lukuo/myik/#p=65.

ROK Ministry of Science and ICT (2022), 'Korea to announce national strategy to become a technology hegemon', https://www.msit.go.kr/eng/bbs/view.do?mId=4&bbsSeqNo=42&nttSeqNo=746.

ROK Ministry of Science and ICT (2023), 년도 착수 민군겸용기술개발사업 기술수요조사 공고 [machine translation: 2024 Commencement of Civil-Military Technology Development Project Technology Demand Survey Announcement], https://www.msit.go.kr/bbs/view.do?nttSeqNo=3178183&bbsSeqNo=100&mId=129&mPid=224.

ROK Ministry of Science and ICT (2023), 'Taking a leap toward becoming a world-leading science and technology hub', https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&bbsSeqNo=42&nttSeqNo=925.

ROK Ministry of Science and ICT (2024), 'MSIT Unveils First Master Plan for Developing Critical and Emerging Technologies (2024-2028): A Blueprint for National S&T Sovereignty', https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&bbsSeqNo=42&nttSeqNo=1034.

Sagamore Institute (2024), 'Defense Tech Investments', https://sagamoreinstitute.org/defense-tech-investments/.

Sang-ho, S. (2022), 'S. Korea aims for 5 pct share in global arms market by 2027', Yonhap News Agency, https://en.yna.co.kr/view/AEN20221124007300325.

Science Japan (2023), 'The Cabinet Office's K Program adds 23 various and advanced projects in its "2nd Vision" based on reports from JST/CRDS', https://sj.jst.go.jp/news/202309/n0912-01k.html.

Shiraishi, S. (2024), 'Japan's Economic Security Policy', Konrad Adenauer Stiftung, https://www.kas.de/en/web/japan/single-title/-/content/japan-s-economic-security-policy-2.

Tesi (2024), 'Finnish defence industry growing strongly, investors eyeing dual-use products in particular', News, https://tesi.fi/en/press-release/finnish-defence-industry-growing-strongly-investors-eyeing-dual-use-products-in-particular/.

Tesi (2024), *Defence: Market study on Finnish military product and dual use companies*, https://tesi.fi/wp-content/uploads/2024/09/Tesi-Defence-Study-240902.pdf.

The People's Government of Fujian Province (2021), 'Outline of the 14th Five-Year Plan (2021-2025) for National Economic and Social Development and Vision 2035 of the People's Republic of China', https://www.fujian.gov.cn/english/news/202108/t20210809_5665713.htm.

The People's Republic of China State Council (2021), 'Outline of the 14th Five-Year Plan for National Economic and Social Development of the People's Republic of China and the Long-Range Objectives Through the Year 2035', https://www.gov.cn/xinwen/2021-03/13/content_5592681.htm.

UK Cabinet Office (2020), National Security and Investment Act 2021, https://www.gov.uk/government/collections/national-security-and-investment-act.

UK Cabinet Office (2021), *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy*, https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

UK Cabinet Office (2023), *Integrated Review Refresh 2023: Responding to a more contested and volatile world*, https://www.gov.uk/government/publications/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world/integrated-review-refresh-2023-responding-to-a-more-contested-and-volatile-world.

UK Department for Science, Innovation and Technology (2023), *The UK Science and Technology Framework*, https://www.gov.uk/government/publications/uk-science-and-technology-framework/the-uk-science-and-technology-framework.

UK Export Control Joint Unit (2024), 'Export controls applying to academic research', Guidance, https://www.gov.uk/guidance/export-controls-applying-to-academic-research.

UK Government (n.d.), 'jHub Defence innovation', https://www.gov.uk/government/organisations/jhub-defence-innovation.

UK Ministry of Defence (n.d.), 'Defence Academy of the United Kingdom', https://www.da.mod.uk/.

UK Ministry of Defence (2019), 'The Defence and Security Accelerator', https://www.oecd-opsi.org/wp-content/uploads/2019/05/650430_9912845_Accelerator-brochureLR-2.pdf.

UK Ministry of Defence (2019), *Defence Innovation Priorities*, https://www.gov.uk/government/publications/defence-innovation-priorities.

UK Ministry of Defence (2021), *Defence and Security Industrial Strategy: A strategic approach to the UK's defence and security industrial sectors*, https://www.gov.uk/government/publications/defence-and-security-industrial-strategy.

UK Ministry of Defence (2024), 'Ministry of Defence funds 2 new Centres for Doctoral Training', News story, https://www.gov.uk/government/news/ministry-of-defence-funds-2-new-centres-for-doctoral-training.

UK Ministry of Defence (2024), *Defence Industrial Strategy - Statement of Intent*, https://www.gov.uk/government/publications/defence-industrial-strategy-statement-of-intent/defence-industrial-strategy-statement-of-intent.

UK Ministry of Defence (2024), *DASA Annual Review 2023-2024*, https://www.gov.uk/government/publications/dasa-annual-review-2023-24.

UK Office for National Statistics (2024), 'Research and development expenditure by the UK government: 2022', https://www.ons.gov.uk/economy/governmentpublicsectorandtaxes/researchanddevelopmentexpenditure/bulletins/ukgovernmentexpenditureonscienceengineeringandtechnology/2022.

UK Parliament (2022), 'Advanced Research and Invention Agency', Statement, https://questions-statements.parliament.uk/written-statements/detail/2022-07-19/hcws218.

UK Parliament (2023), 'National Security Strategic Investment Fund', Question for Department for Business and Trade, https://questions-statements.parliament.uk/written-questions/detail/2023-11-24/3591/.

UK Research and Innovation (2023), '2022-23 — 2024-25 budget allocations for UK Research and Innovation', https://www.ukri.org/wp-content/uploads/2022/06/UKRI-241023-BudgetAllocationExplainer2022To2025.pdf.

University of Wisconsin – Green Bay (n.d.), 'Export Controls', Office of Grants & Research, https://www.uwgb.edu/research/research-compliance-and-training/export-controls/.

U.S. Bureau of Industry and Security (n.d.), 'About Export Administration Regulations (EAR)', https://www.bis.gov/regulations.

U.S. Department of Defence (n.d.), 'Defense Innovation Board – Our Story', https://innovation.defense.gov/About1/.

U.S. Department of Defence (2022), *2022 National Defense Strategy of the United States of America*, https://www.defense.gov/National-Defense-Strategy/.

U.S. Department of Defence (2024), *The Defense Innovation Unit FY 2023 Annual Report*, https://downloads.ctfassets.net/3nanhbfkr0pc/57VfnQbajgWdONRicxv6nG/44f831e7a0e857bb8494508f8571fd71/DIU_Annual_Report_FY2023.pdf.

U.S. Department of Defence (2024), 'Fiscal Year (FY) 2025 Budget Estimates', https://www.darpa.mil/sites/default/files/attachment/2024-11/u-rdte-mjb-darpa-pb-2025-06-mar-2024-final.pdf.

U.S. Department of Defence Innovation Marketplace (n.d.), 'Long-Range Research and Development Program Plan', https://defenseinnovationmarketplace.dtic.mil/innovation/long-range-research-development/.

U.S. Department of Energy (n.d.), 'Office of Critical and Emerging Technologies', https://www.energy.gov/cet/office-critical-and-emerging-technologies.

U.S. Department of State (n.d.), 'Office of the Special Envoy for Critical and Emerging Technology', https://www.state.gov/bureaus-offices/secretary-of-state/office-of-the-special-envoy-for-critical-and-emerging-technology/.

U.S. Department of the Treasury (n.d.), 'CFIUS Overview', https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview.

U.S. Federal Government (2013), Executive Order 13637—Administration of Reformed Export Controls, https://www.govinfo.gov/content/pkg/DCPD-201300143/pdf/DCPD-201300143.pdf.

U.S. Federal Government (2025), Federal Acquisition Regulation, https://www.acquisition.gov/browse/index/far.

U.S. Federal Government (2025), Defense Federal Acquisition Regulation Supplement, https://www.acquisition.gov/dfars.

Whorwood, H., Robinson, D., and Hyde, F. (2024), 'UK Defence Tech 2024: Advancing National Security through Innovation', Beauhurst and MD One Ventures, https://www.beauhurst.com/wp-content/uploads/2024/05/Beauhurst-UK-Defence-Tech-2024.pdf.

World Bank (n.d.), 'GDP (current LCU) - United States', https://data.worldbank.org/indicator/NY.GDP.MKTP.CN?locations=US.

World Bank (n.d.), 'GDP (current LCU) - China', https://data.worldbank.org/indicator/NY.GDP.MKTP.CN?locations=CN.

World Bank (n.d.), 'Research and development expenditure (% of GDP) - China', https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS?locations=CN.

World Bank (n.d.), 'Military expenditure (% of GDP) – China' (n.d.), https://data.worldbank.org/indicator/MS.MIL.XPND.GD.ZS?locations=CN.

World Bank (n.d.), 'GDP (current LCU) - Korea, Rep.', https://data.worldbank.org/indicator/NY.GDP.MKTP.CN?locations=KR.

World Bank (n.d.), 'GDP (current LCU) - United Kingdom', https://data.worldbank.org/indicator/NY.GDP.MKTP.CN?locations=UK-GB.

World Bank (n.d.), 'GDP (current LCU) – Israel', https://data.worldbank.org/indicator/NY.GDP.MKTP.CN?locations=IL.

World Bank (n.d.), 'Military expenditure (current LCU) – Israel', https://data.worldbank.org/indicator/MS.MIL.XPND.CN?locations=IL.

Zhu, B. C., Rao, D., Xie Y., and Li, N. (2024), 'China's New Export Control Framework: Key Changes for Dual-Use Items', Morrison Foerster, https://www.mofo.com/resources/insights/241216-china-s-new-export-control-framework-key-changes.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union.
You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

Recognising the importance of dual-use technologies as well as the challenges specifically related to their implementation in EUfunded projects, this report offers insights with concrete examples and case studies on how dual-use research and innovation can work in practice. It provides evidence and facts on opportunities and challenges related to civil-defence synergies; it uncovers practical implementation of dual-use research and innovation within the perspective of research performing organisations and small and medium-sized enterprises, start-ups and scale-ups; and puts forward international examples and benchmarks on policy strategies and funding programmes supporting dual-use research and innovation.

Research and Innovation policy

Publications Office
of the European Union