



Royal Academy
of Engineering

Understanding Dual-Use:

Concepts, Tensions
and Trade-offs

About this paper

This paper does not seek to resolve the challenges associated with dual-use technologies or to prescribe a single approach. Instead, it aims to surface how the term is currently applied in practice and to highlight the tensions and trade-offs that appear across research, innovation, economic and security contexts.

By setting out how technologies can be interpreted and governed in different ways, the paper draws attention to the risk of inconsistent or contradictory outcomes when competing objectives are not made explicit. Its primary purpose is to encourage policymakers to recognise these tensions more clearly and to consider the wider system impacts of their decisions.

It is worth noting that the purpose of this paper evolved over time. While initial work focused on clarifying the definition of dual-use, engagement with stakeholders revealed a broader challenge that moved beyond terminology to consider how competing policy objectives are balanced in an increasingly complex technological and geopolitical landscape.

Summary

Dual-use is a term broadly applied to items with both civilian and military applications. It is being increasingly used amid geopolitical tensions and technological advancement. Both exploitation and protection of dual-use technologies has become a priority for national security and economic policy. Despite widespread use, its meaning often shifts depending on context, community and purpose. Differing uses within one conversation were observed at a meeting of Royal Academy of Engineering National Security Fellows, for example. We set out to explore how the term is applied in practice

and whether a shared understanding is needed. We conducted desk-based research and interviews with a few key stakeholders.

This paper summarises what we learned: how the term is understood and applied; where inconsistencies arise and how these reveal wider policy tensions. It offers a set of potential options for a shared understanding of dual-use and poses wider questions about whether a broader discussion on technology, defence, national security, resilience, and economic growth is needed.

A brief history of the term 'dual-use'

page 4

Governing dual-use items

page 7

Inherent tensions

page 10

Towards clarity, coherence and consensus

page 12

Fresh thinking

page 14

Annex 1

page 15

A brief history of the term 'dual-use'

In the 1940s, military and civilian items were largely distinct and separate entities. Items considered 'military' included bombs, guns and tanks, while those considered 'civilian' encompassed almost everything else. Instances of overlap between these two categories were relatively few and far between. Post-WWII, with the nuclear arms race in full swing, nuclear materials emerged that could be used for the development of weapons of mass destruction (military), but also for the production of nuclear power (civilian). This was the first application of the term 'dual-use',¹ that is, an item with both civilian and military applications. It was applied in specific contexts relating to control and protection in aid of defence and national security objectives. WWII similarly saw the development of radar, which led to major advances in electronic engineering and later benefited everyday household technologies. War, because of its urgent and strategic demands, often accelerates innovation, much of which inevitably diffuses into the civilian sector. WWII was an especially productive period for technological development.

The current landscape is far more complex. Technologies have proliferated and innovation happens at pace. Military innovation is no longer solely driven by the government, with a larger proportion of innovation coming from the commercial sector before being adopted into defence acquisition pipelines. This means that ideas do not always emerge from government programmes, but increasingly

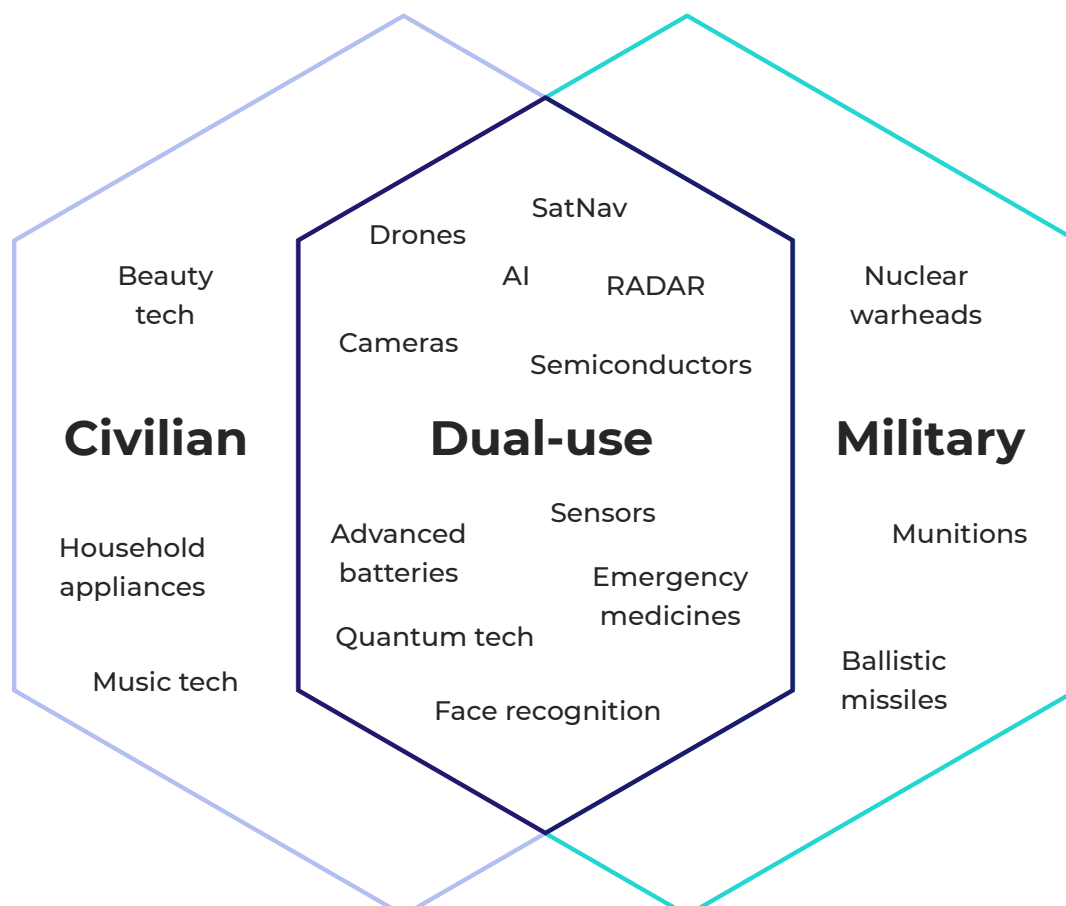
from private, commercial actors. Lines between civilian and military applications have become increasingly blurred, with items ranging from hobbyist drones to cloud computing software considered dual-use, with visible applications in Ukraine. The concept of dual-use has expanded so much that military applications are now only one consideration among many, with broader national security considerations such as resilience, sovereignty, and cyber- and economic security all now in play. For instance, the European Parliament cite dual-use export controls as "tools for EU economic security."² The picture is further complicated by the fact that the concept of economic security is not clearly defined. A recent Business and Trade Committee inquiry noted that 'economic security' has no accepted definition despite being attached to a range of different policy areas including defence and trade.³ For some, it concerns the protection of a country's competitiveness and economic interests. Others use it to refer to access to the resources and underlying supply chains needed to sustain prosperity and national security. It is also used as a broader term that considers employment, standards of living and resilience to inflation. The Committee cites this causing difficulty and a lack of clear understanding within government. Similarly, spending ringfenced for 'resilience' came under scrutiny at a recent National Security Strategy Committee session because of the lack of a clear definition, which can encompass everything from flood protection to undersea cables to information security.⁴

Defining and governing dual-use items is further complicated when considering components rather than discrete systems. Technologies are constructed from tens, hundreds and even thousands of discrete components, each with its own risk profile, supply chain and applications. As the concept of dual-use has expanded, the number of components captured within its scope is vast. Semiconductors are a prime example of this: these are used in computing, communication, transportation, clean energy, and for battlefield technologies.

Dual-use platform digital technologies such as cloud infrastructure, foundational AI models, computational simulations, and large-scale data systems require distinct

treatment: they are neither traditional components nor discrete systems with fixed end-uses. A single model used to accelerate drug discovery, for instance, could be applied to accelerate weapons design, placing it firmly under the dual-use umbrella. However, as intangible technologies, they cannot be governed in the same way as physical goods. Assessing risk is further obscured by the fact that platform technologies can shift rapidly, whether through fine-tuning that alters model behaviour or through novel, malicious uses. These technologies do not adhere to traditional innovation cycles. They emerge quickly and evolve continuously. While physical goods can be identified and controlled at borders, platform technologies

Figure 1: Venn diagram illustrating widening scope of dual-use technologies as compared to purely military or purely civilian technologies. Examples are illustrative. While this illustration focuses on discrete technologies and systems, similar considerations increasingly apply to enabling infrastructure, particularly in areas such as energy and communications.



cannot. As a result, control becomes a matter of regulating access and considering specific application areas rather than transfer.

These examples illustrate how both the range of technologies captured and the contexts in which the term is applied continues to expand. It is now used not only in the context of risk mitigation, but in reference to economic growth, with the UK government explicit in its ambition to scale civilian applications of defence Intellectual Property (IP), and to transfer civilian innovations into defence markets. For instance, the Defence and Economic Growth Taskforce⁵ (DETF), has been tasked to provide recommendations to government on ‘identifying and scaling dual-use opportunities’ in the defence acquisition pipeline with potential commercial applications and vice-versa to broaden the potential market base for dual-use items. This adds further ambiguity to the concept.

At the other end of the development pipeline sits academic research, an additional dimension to the dual-use challenge. Where research is directly applicable to defence, there are obvious requirements for certain protections and controls. The risks become harder to identify in earlier stage research that may not be initially intended for defence but might have dual-use potential. A prime example of this is research into emergency medicine. Medical capability has long been a core component of military strategy. The capacity to save injured soldiers and return them to the battlefield can be as strategically important as the weaponry itself. However, emergency medicine research is also being used to identify which wounds are most difficult to treat, with findings informing weapon design to maximise harm. In this sense, emergency medicine research may be considered dual-use and therefore be subject to protective measures. Treating weapons research and lifesaving medical research as

equivalent under the dual-use label, however, fails to account for the ethical distinction between taking and saving lives. This is further complicated by an environment that follows the norms of open science, peer review, collaboration, and the international flow of talent, especially when considering the long strategic time horizons of adversaries who may see foundational research, even at the conceptual stage, with future security and military advantage in mind.

A speech by the former UK Science Minister Lord Patrick Vallance emphasised the importance of cautious, sensible and informed international science cooperation in the context of the UK–China relationship, arguing for an approach that upholds academic freedom while being clear-eyed about areas of disagreement and risk. This illustrates the level of nuance required when navigating these tensions in public and in policy, where a fine line must be navigated between providing partners with certainty, while preserving our ability to continuously consider the threats to national security that collaboration on dual-use research could pose.

These factors combined illustrate that the concept of dual-use has evolved beyond the relatively bounded meaning it once held. What once referred primarily to discrete items is now used to describe a far broader landscape encompassing hardware, software, components, research, knowledge, and enabling infrastructure. The term increasingly struggles to distinguish where genuine risks and opportunities lie, or to provide a stable basis for aligned policy action. When a single term is stretched so tightly, it risks ceasing to be a useful tool for judgement altogether. This raises the more fundamental challenge of whether the existing framing can support clear and proportionate decision-making, or if an alternative approach is needed.

Governing dual-use items

Existing national measures

The government relies heavily on innovation outside the defence sector to boost defence capabilities. This dynamic exists in an environment more competitive, contested and strategically volatile than at any point since the end of the Cold War in the mid-1990s. Returns on investment in solely military technologies can be dependent on external unpredictable factors and is often conditional on government funding if there is not a sizeable commercial outlet that can sustain the business in periods of peace. The government is therefore looking to leverage the commercial sector to procure and develop dual-use items to boost their military capabilities. This strategic reliance on dual-use items means we are seeing it appear both in government strategy documents where it is largely undefined, and in regulations and legal frameworks where it is more explicitly described.

UK government strategies and funds

For example, the government is rolling out a series of policy initiatives and measures that drive investment and leverage dual-use items for economic growth:

- The National Security Strategic Investment Fund (NSSIF), established in 2018, acts as the government's venturing arm which backs

'pioneering dual-use technologies with both commercial and strategic potential'.⁶

- The government has committed 10% of the Ministry of Defence (MOD) budget to supporting dual-use innovation.⁷
- The Strategic Defence Review⁸ promises a new Defence Exports Office 'to drive exports to our allies and growth at home'.
- The UK has a system of state support geared towards fuelling dual-use innovation at all stages. UK Defence Innovation⁹ is the main vehicle for this, with the Defence and Security Accelerator being the entry point for dual-use ideas, welcoming civilian-first technologies without a pure defence case. Innovate UK also has funds for commercial innovation with potential defence relevance.

UK regulation

In parallel, several legal and regulatory frameworks exist to identify and regulate dual-use items because of the risks they pose:

- The National Security and Investment Act (NSIA)¹⁰ provides powers to scrutinise business transactions involving sensitive capabilities. It identifies 17 sensitive areas of the economy where mandatory notification is required for certain acquisitions. One of these areas is explicitly 'Military and Dual-Use', however the other 16 could also be

considered dual-use by many interpretations, especially when considering resilience and economic security objectives. NSIA's purpose is to both monitor foreign acquisitions that threaten our national security and keep track of UK-developed IP being absorbed by foreign investor firms.

- The Academic Technology Approval Scheme (ATAS) monitors risks by applying controls to certain foreign students and researchers working in specific sensitive fields.¹¹ While ATAS does not use the term 'dual-use' explicitly, its purpose aligns with dual-use concerns: preventing the transfer of knowledge that could be applied to military or proliferation activities.

These legal and regulatory frameworks were each developed for a specific discrete purpose, not in concert and are now applied more widely than initially designed.

University guidance and assurance frameworks (NPSA and NCSC)

In addition to formal regulation, universities and research organisations rely heavily on guidance from the National Protective Security Authority (NPSA)¹² and the National Cyber Security Centre (NCSC)¹³ to support policy, risk assessment and assurance. NPSA's Trusted Research guidance, including the Trusted Research Evaluation Framework, is used to help institutions identify and manage risks associated with international research collaboration. This guidance is increasingly embedded in government processes. For example, participation in MOD initiatives such as the Defence Universities Alliance requires institutions to demonstrate alignment with NPSA trusted research principles. These frameworks play a central role in shaping how dual-use risks are interpreted and managed in academic settings.

Existing international measures

The dual-use challenge is inherently international because it is the cross-border flow of technology that enables proliferation. An international approach that is aligned with partners and equally clear-eyed on the behaviour of non-allied nations is therefore crucial for effective governance.

Export controls

Export controls are the primary and most powerful mechanisms through which governments can control the flow of dual-use technologies. They establish legal requirements before certain items can be exported. The current legislation defines dual-use items as goods, software and technology that can be used for both civilian and military purposes. Recent amendments have extended the scope to include emerging technologies such as quantum computing, AI and semiconductor manufacturing equipment, which reflects the expansive nature of the dual-use concept.

UK export control policy is heavily shaped by international and multinational governance agreements. The UK consolidated list of strategic military and dual-use items is not developed in isolation, it is the product of continuous negotiations with allied nations and is regularly updated, often based on international export control regimes and agreements. Some key examples include:

- **Wassenaar Arrangement**¹⁴
A multilateral export control regime focusing on conventional arms and dual-use goods, which leads to negotiated agreements for export controls.
- **International Traffic in Arms Regulations (ITAR)**¹⁵
A US regulatory framework governing

export of defence related articles and services. While this is national, it has significant extraterritorial impact. ITAR is frequently used to protect US companies for economic advantage as well as protecting technologies with military applications. This means it can constrain collaboration between UK and US organisations, as any technology or IP may remain subject to US export controls. ITAR controls may also apply retrospectively to previously unrestricted work.

- **Australia Group**¹⁶

An informal cooperation framework that seeks to prevent the spread of chemical and biological weapons by harmonising export controls on precursor chemicals, biological agents and related equipment.

- **Chemical Weapons Convention (CWC)**¹⁷

A legally binding treaty prohibiting the development, production, stockpiling, and use of chemical weapons.

- **Zangger Committee**¹⁸

A group that supports the Nuclear Non-Proliferation Treaty by providing guidance on which nuclear materials and technologies require export controls.

It is worth reiterating that platform digital technologies cannot be effectively controlled under most existing export control agreements. Physical goods can be intercepted at borders whereas platform technologies cannot, so traditional controls struggle to address intangible technologies. There have been a limited number of attempts to tackle this:

- **US Bureau of Industry and Security (BIS) semiconductor export controls**

The most deliberate attempt to regulate at the platform layer. The October 2023 rules and further iterations seek to constrain foundational AI capabilities indirectly by controlling the semiconductor hardware and compute infrastructure on which they depend.¹⁹

- **Wassenaar Arrangement**

This agreement has made some efforts to incorporate emerging and digital technologies into its control lists. In 2013, controls on 'intrusion software' were introduced,²⁰ however this exposed the limits of attempting to shoehorn intangible technologies into an existing hardware-focused framework. Progress is slow and consensus-based, with decisions taking months to years, far slower than innovation cycles in digital technologies.

- **Pall Mall Process**²¹

An international initiative launched by the UK and France in 2024 to address the proliferation and misuse of commercial, intangible cyber intrusion capabilities, including spyware and hacking services. It focusses on improving oversight and creating controls on the sale of software, rather than banning them outright. However, participation is nonbinding, with no enforcement or sanctions mechanism. This raises questions about its effectiveness.

This suite of examples illustrates the different lenses through which the same dual-use item could be considered, and how different mechanisms could apply depending on context. Taken together, it signals a serious strategic and financial commitment to both seizing the potential economic advantages and mitigating the security risks associated with dual-use technologies. But it also highlights conflicting objectives and the tension between openness and protectionism – nuance is required to determine in what contexts we should be seeking to openly scale or protect and control the expanding pool of dual-use research, items and technologies.

Inherent tensions

As it stands, dual-use items are being pulled in different directions to be leveraged for different, legitimate policy objectives, some complementary, some contradictory. If, say, the Department of Business and Trade (DBT) seeks to scale a home-grown hobbyist drone business by supporting access to international civilian markets, this would deliver economic benefit. However, the MOD could argue that this risks proliferation of a dual-use technology to non-allied states that could misuse it in ways that threaten our national security, and so protection and domestic procurement by our military is the best course of action. This intentionally simplistic example illustrates how departments, acting rationally and within their remits, could end up working against each other.

The tensions and conflicting objectives can result in contradictory outcomes, as illustrated by the following use cases:

- It was reported to us that a student working on improving train performance successfully received ATAS approval. The same researcher later applied for a postdoctoral position, requiring a new ATAS approval for a follow-on study. This time, the study title was more specific about the methods. This application was rejected because of its dual-use potential, despite the underlying work and objectives being the same. In this case, differences in

wording and framing led to an altogether different judgement of the risks posed rather than a change in underlying risk.

- We have also been made aware of cases where students from non-allied countries have been granted ATAS approval in nonsensitive disciplines before later seeking to move into areas with clear dual-use implications, such as quantum technologies. This demonstrates how adversaries may attempt to circumvent approval processes in ways that could undermine safeguards.
- Two of the five prohibited transactions under the NSIA related to dual-use potential. The first blocked a licence agreement between the University of Manchester and Beijing Infinite Vision Technology Company Ltd, due to the nature of the IP having dual-use potential. Later that same year, the government blocked Hong-Kong based firm Super Orange HK Holding Ltd due to the design automation technology having potential dual-use applications.²² There is no indication that the government then stepped in to assist in securing alternative investment in either of these cases. As a result, interventions designed to protect national interests could constrain commercialisation and domestic scaling of goods with economic potential.

- In May 2022, the government significantly tightened its military end-use controls, particularly in relation to China. This change was not concerned with banning additional goods, but about how risk is assessed. Under the new rules, the UK may require an export licence for *any* item (that is, items beyond those on the UK Strategic Export Control Lists) if there is suspected military end-use, or a suspected military end-user. Another example is the EU banning the export of cement mixers to Russia following its invasion of Ukraine in April 2022, because it became clear that they were being used to manufacture storage facilities for nuclear missiles. Cement mixers are not typically considered dual-use goods in the traditional sense, where an item has inherent characteristics that lend themselves to both civilian and military applications. However, this case illustrates a broader shift in export controls, where items can be treated as if they were dual-use based on their anticipated end-use. Controls in this context are no longer defined solely by the intrinsic properties of goods, but instead by the risks associated with how and by whom they are used. While this provides flexibility to respond to emerging threats, it also means that the same goods could be unrestricted in one context and prohibited in another.

It is apparent that the challenge of defining and governing dual-use is a microcosm of a larger set of inherent tensions between key government policy objectives of national security, economic security, economic growth, and sovereignty. Navigating these tensions involves not just categorising technologies by their dual-use potential but managing a system in which similar technologies and activities could be simultaneously enabled and constrained depending on context. Without shared frameworks for judgement, well-intentioned interventions could end up working against each other.

Towards clarity, coherence and consensus

The dual-use challenge is complex and evolving. New technologies emerge at pace, geopolitical events continually alter the landscape of risk and opportunity, and there is a broad and diverse set of stakeholders with differing incentives. Policymakers, investors, SMEs, researchers, militaries, and regulatory bodies all have a stake in seizing opportunities, mitigating risks, or both. Each group brings its own priorities and responsibilities, and varying levels of technical knowledge on the technologies with which they are tasked to govern. Each needs confidence and clarity on how best to proceed, and a coordinating body able to straddle the military and civilian worlds would be crucial for ensuring ownership and quick responses to emerging technological threats.

Below we set out some options for consideration to move towards clarity, coherence and consensus. The Academy is well positioned to act as a neutral convener, bringing together stakeholders across sectors who may be grappling with these challenges in isolation. We consider if there is a need to broaden the discussion to explore the tensions and trade-offs between different government objectives. The stakeholders we have consulted thus far have all expressed an appetite for surfacing tensions and a wider discussion on the UK's approach to technology governance across the various contexts in which it is applied.

Many different stakeholders pursue legitimate but diverse objectives that each

consider dual-use items in distinct ways. To support a more coherent approach, shared analytical tools and frameworks can help stakeholders map and visualise potential trade-offs, risks and opportunities to manage competing priorities which may require different approaches. These tools are not designed to guarantee the same outcome across stakeholders. Instead, they add an element of standardisation to the decision-making process.

Tool 1: a dual-use recognition spectrum

A linear spectrum placing dual-use items along the Research and Innovation (R&I) pipeline, from concept through to deployment. This would highlight when and where dual-use potential emerges and when governance, export control or commercialisation decisions should apply. This could draw on the Technology Readiness Level model, which is already widely understood and routinely applied across the R&I system. Stakeholder responsibility zones could highlight who should act at each stage. A similar spectrum has been proposed by CESAER, a European association of over 50 leading universities of science and technology, for considering dual-use projects in EU-level funding programmes.²³

Tool 2: a policy trade-off matrix

A matrix mapping different scenarios against policy objectives, such as economic growth, sovereignty and security, with each cell illustrating whether a decision represents a trade-off, a win-win or a lose-lose. For instance, for a hypothetical policy such as tighter export controls, the cell corresponding to security and growth might show a trade-off, reflecting security gains (because of less export of items that could be used against us) but constrained economic growth (because of limited international trade). This tool could reveal wider consequences of policy choices and highlight where tensions lie.

intervention points for meaningful change. This would involve a workshop to map the key people, organisations and stakeholders, alongside the processes, responsibilities and behaviours that shape their decision-making.²⁵ This could help decision-makers better visualise where hidden interdependencies and bottlenecks appear to help them understand and navigate the complexity of the landscape. Considering the different, and sometimes distant, stakeholders within the system could encourage more coordinated and joined-up action.

It is worth noting that these options are geared towards tangible technologies and would not be appropriate for platform digital technologies. Governing intangible technologies would require an altogether different approach.

Tool 3: a civil-military advantage quadrant

A quadrant chart categorising technologies by their sector of origin and dominant advantage sector (civilian v military). This could act as a tool for understanding how dual-use technologies move between sectors and which interventions are most appropriate. Royal United Services Institute (RUSI) have proposed a similar model, which analyses innovation at the component level and categorises by the origin of the component and the length of the innovation cycle. Each quadrant therefore has distinct characteristics and institutional requirements.²⁴

A systems approach

Responsibility for developing, governing and stewarding dual-use technologies sits across multiple government departments, industries, regulatory regimes, and R&I ecosystems, all of which have distinct priorities, processes and incentives. The interaction between these systems creates interdependencies and unknowns. Systems approaches can support better informed decision-making and encourage consideration of different perspectives. This helps policymakers as well as technology researchers and developers to better understand how complex, adaptive systems behave and interact, which supports effective action while reducing consequences that negatively affect other parts of the system. This is particularly valuable when tackling challenges where there are blurred lines of responsibility and accountability. This is a core component of the dual-use challenge.

Tool 4: Participatory Systems Mapping exercise

A Participatory Systems Mapping exercise is used to identify how different systems that seek to govern and steward dual-use technologies, for instance research, innovation, procurement, and international trade, interact in practice to identify

Fresh thinking

The tensions identified in this paper reveal not just the complexity of modern technologies, but the complexity of the governmental system that is tasked with managing them. It demands clear and aligned action across the whole system to ensure risk and opportunity are balanced effectively and in line with government objectives. Our current approach relies on assumptions that once held true when military and civilian items were distinct, but this distinction no longer holds. Technological development is now advancing rapidly and in many directions at once.

This evidence gathering exercise has exposed deeper policy tensions that stretch far beyond questions of terminology and categorisation. Addressing these tensions demands much broader conversations about the UK's approach to national security, economic policy and sovereignty. Dual-use as a label should signal where these policy objectives may be pulling in different directions. This indicates that decisions could have distant consequences beyond their immediate context, and so may require deeper examination and active engagement with relevant internal and external stakeholders. Recommendations are deliberately not included in this paper. The Academy cannot resolve the tensions inherent in dual-use, but has sought to bring them out into the open and encourage further discussion.

Annex 1

Objective	Stakeholder	Action	Potential risks	Potential opportunities
Boost economic growth	DBT – Economic Growth team	Attract foreign investment Promote global partnerships Fast-track commercialisation of emerging tech	Increased foreign influence IP leakage Dependency on non-allied supply chains	Economic growth Attract international talent
Protect UK economic resilience and sovereignty	DBT – Economic Security team	Incentivise domestic manufacturing and reshoring Impose export controls Secure supply chains through subsidies	Reduced competitiveness Retaliation from trade partners Slower innovation	Military / strategic advantage Reduced reliance on international supply chains Strengthen sovereign capabilities
Ensure the UK is well-equipped to defend itself	Military	Procure cutting-edge tech rapidly Collaborate with top-tier suppliers	Supply chain and security vulnerabilities	Military advantage Procurement of best-in-class technologies
Maintain sovereign military capabilities and achieve strategic advantage	MOD	Fund classified projects Seek partnership with leading defence firms Accelerate R&I	Tech leakage Reliance on foreign defence firms	Procurement of best-in-class technologies Accelerated innovation cycles
Combat and reduce threats to our national security	Agencies	Impose control on sensitive tech Prioritise protectionism / secrecy Block risky foreign collaborations	Slow innovation Diplomatic tension Reduced global competitiveness	Military / strategic advantage

Objective	Stakeholder	Action	Potential risks	Potential opportunities
Ensure R&I excellence, and financial sustainability	University	- Seek funding from investors, including foreign firms and governments - Collaborate with world-leading institutions - Attract global talent - Publish widely - Oppose policies that limit innovation - Advocate for open science and global knowledge exchange	- IP leakage - Foreign influence in research agendas - Misuse of home-grown research	- Attract international talent - Increased quality of research - Deeper, broader research system - Maintain status as world-leader in research
Conduct impactful, well-funded research	Researcher	- Accept grants from any source - Share results openly for maximum impact - Publish in the most prestigious journals - Prioritise high-impact publications	- Proliferation of sensitive dual-use research and knowledge - Foreign influence in research agenda - Reputation risk if research is misused	Contribute skills, talent and knowledge to national security objectives
Scale and grow their companies	SME owner	- Quickly enter new, global markets - Accept foreign investment - Outsource production to reduce costs	- IP leakage - Dependency on non-allied states - Foreign influence in innovation processes	- Boost UK economy - Attract international talent
Maintain competitiveness and support allied defence capabilities	Large defence corporates	- Secure government contracts - Invest in R&D - Export products to allied nations - Develop and commercialise into both commercial and defence sectors	- Technology proliferation - Misuse of dual-use technologies - Reputational risk	- Economic growth - Military advantage - Innovation gains for the commercial sector - Strong domestic defence capabilities

Objective	Stakeholder	Action	Potential risks	Potential opportunities
Promote tech leadership and innovation	Department of Science, Innovation & Technology	Encourage commercialisation Support global R&I networks	Uncontrolled proliferation of sensitive tech Weakened export controls	Strengthened R&I ecosystem Strengthen relationships with international research partners
Maximise returns	Investors	Invest in high-growth companies (regardless of origin) Prioritise growth and global expansion Seek quick returns on their investments	Investment in firms linked with non-allied nations Proliferation of dual-use innovation	Boost economic growth More investment in dual-use space will drive skills and employment in the area (and so strengthen sovereign capabilities)
Enable interoperability of regulations and standards	Standards bodies	Develop standards that align with international frameworks Balance speed to market with appropriate security measures	Standards misaligned with security needs Stifling of economic growth if too bureaucratic and stringent Threatening to national security if too lenient	More clarity for researchers, entrepreneurs and policymakers

References

- 1 MIT Dual-Use Readiness Model. (n.d.) *Defining “Dual-Use”*. Retrieved 21 May 2026 from dualuse.mit.edu/defining-dual-use/
- 2 European Parliament. (2025) *Dual-use export controls as tools of EU economic security: From coordination to a proactive EU approach.* Retrieved 21 May 2026 from [www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2025\)777960](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)777960)
- 3 UK Parliament. (2025). *Toward A New Doctrine For Economic Security, Eleventh Report of Session 2024–26.* Retrieved 21 May 2026 from publications.parliament.uk/pa/cm5901/cmselect/cmbeis/835/report.html
- 4 UK Parliament. (n.d.) *The National Security Strategy - Oral evidence.* Retrieved 21 May 2026 from committees.parliament.uk/committee/111/national-security-strategy-joint-committee/publications/oral-evidence/
- 5 CBI. (n.d.) *UK Defence and Economic Growth Taskforce.* Retrieved 21 May 2026 from www.cbi.org.uk/our-work/defence-taskforce/
- 6 *National Security Strategic Investment Fund.* (n.d.) *Investing in the future security and prosperity of the UK.* Gov.UK. Retrieved 21 May 2026 from www.nssif.gov.uk/
- 7 Ministry of Defence. (2025). *Defence Industrial Strategy 2025: Making Defence an Engine for Growth.* Gov.UK. Retrieved 21 May 2026 from www.gov.uk/government/publications/defence-industrial-strategy-2025-making-defence-an-engine-for-growth
- 8 Ministry of Defence. (2025). *Strategic Defence Review - Making Britain Safer: secure at home, strong abroad.* Gov.UK. Retrieved 21 May 2026 from www.gov.uk/government/publications/the-strategic-defence-review-2025-making-britain-safer-secure-at-home-strong-abroad
- 9 Ministry of Defence (n.d.) *UK Defence Innovation.* Gov.UK. Retrieved 21 May 2026 from www.gov.uk/government/organisations/uk-defence-innovation
- 10 The Cabinet Office. (2026). *National Security and Investment Act 2021.* Gov.UK. Retrieved 21 May 2026 from www.gov.uk/government/collections/national-security-and-investment-act
- 11 Foreign Commonwealth and Development Office. (2026). *Academic Technology Approval Scheme (ATAS).* Gov.UK. Retrieved 21 May 2026 from www.gov.uk/guidance/academic-technology-approval-scheme
- 12 NPSA. (n.d.) *National Protective Security Authority.* Gov.UK. Retrieved 21 May 2026 from www.npsa.gov.uk/

- 13 NCSC. (n.d.) *National Cyber Security Centre*. Gov.UK. Retrieved 21 May 2026 from www.ncsc.gov.uk/
- 14 Wassenaar Arrangement Secretariat (n.d.) *The Wassenaar Arrangement*. Retrieved 21 May 2026 from <https://www.wassenaar.org/>
- 15 US Department of State.(n.d.) *The International Traffic in Arms Regulations (ITAR)*. Retrieved 21 May 2026 from www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=24d528fddbfc930044f9ff621f961987
- 16 The Australia Group. (n.d.) *Fighting the spread of chemical and biological weapons*. Australian Government Department of Foreign Affairs and Trade. Retrieved 21 May 2026 from www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html
- 17 Organisation for the Prohibition of Chemical Weapons. (n.d.) *Chemical Weapons Convention*. Retrieved 21 May 2026 from www.opcw.org/chemical-weapons-convention
- 18 *Zangger Committee*, (n.d.) Zangger Committee. Retrieved 21 May 2026 from zanggercommittee.org/
- 19 U.S. Bureau of Industry and Security. (2023) *Commerce strengthens restrictions on advanced computing semiconductors [...] to countries of concern*. Retrieved 21 May 2026 from www.bis.gov/press-release/commerce-strengthens-restrictions-advanced-computing-semiconductors-semiconductor-manufacturing-equipment
- 20 U.S. Industry and Security Bureau. (2015) *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*. *Federal Register*. Retrieved 21 May 2026 from www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items
- 21 Foreign, Commonwealth and Development (2024) *Pall Mall Process on proliferation and irresponsible use of commercial cyber intrusion capabilities: UK and France joint communiqué*. Gov UK. Retrieved 21 May 2026 from www.gov.uk/government/publications/pall-mall-process-on-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities-uk-and-france-joint-communiqué
- 22 Natalie Yeung. (2022) *Two Deals by Chinese Companies Blocked Under the UK's National Security and Investment Act*. Slaughter and May Retrieved 21 May 2026 from www.slaughterandmay.com/insights/imported-content/two-deals-by-chinese-companies-blocked-under-the-uk-s-national-security-and-investment-act/
- 23 CESAER. (2026) *Clarifying and optimising civil, dual-use and defence research and innovation in future EU funding programmes*. Retrieved 21 May 2026 from www.cesaer.org/news/clarifying-and-optimising-civil-dual-use-and-defence-research-and-innovation-in-future-eu-funding-programmes-2164/
- 24 Mirko Niederkofler. (2025) *Drones win battles, components win wars*. RUSI. Retrieved 21 May 2026 from www.rusi.org/explore-our-research/publications/commentary/drones-win-battles-components-win-wars
- 25 Centre for Evaluation of Complexity Across the Nexus. (2020) *Participatory Systems Mapping: a practical guide*. CECAN. Retrieved 21 May 2026 from www.cecac.ac.uk/wp-content/uploads/2020/09/PSM-Workshop-method.pdf

The Royal Academy of Engineering creates and leads a community of outstanding experts and innovators to engineer better lives. As a charity and a Fellowship, we deliver public benefit from excellence in engineering and technology and convene leading businesspeople, entrepreneurs, innovators and academics from every part of the profession. As a National Academy, we provide leadership for engineering and technology, and independent, expert advice to policymakers in the UK and beyond.

We have three goals:

Sustainable and Innovative Economy, where sustainability drivers, innovative industries and resilient infrastructures are aligned to drive growth and productivity that will support better lives for all.

Technology Improving Lives, where technology in all its forms is used to meet the most important human needs, avoid harm, support fairer societies and break down barriers to opportunity.

Engineering Community Fit for the Future, where our community reflects society in its diversity, commits to creating inclusive cultures to help drive engineering excellence, and has the skills to meet future needs safely, securely and ethically, and to keep pace with innovation.

Our work is enabled by funding from the Department for Science, Innovation and Technology, corporate and university partners, charitable trusts and foundations, and individual donors.

Royal Academy of Engineering
Prince Philip House
3 Carlton House Terrace
London SW1Y 5DG

Tel 020 7766 0600
www.raeng.org.uk

Registered charity number 293074