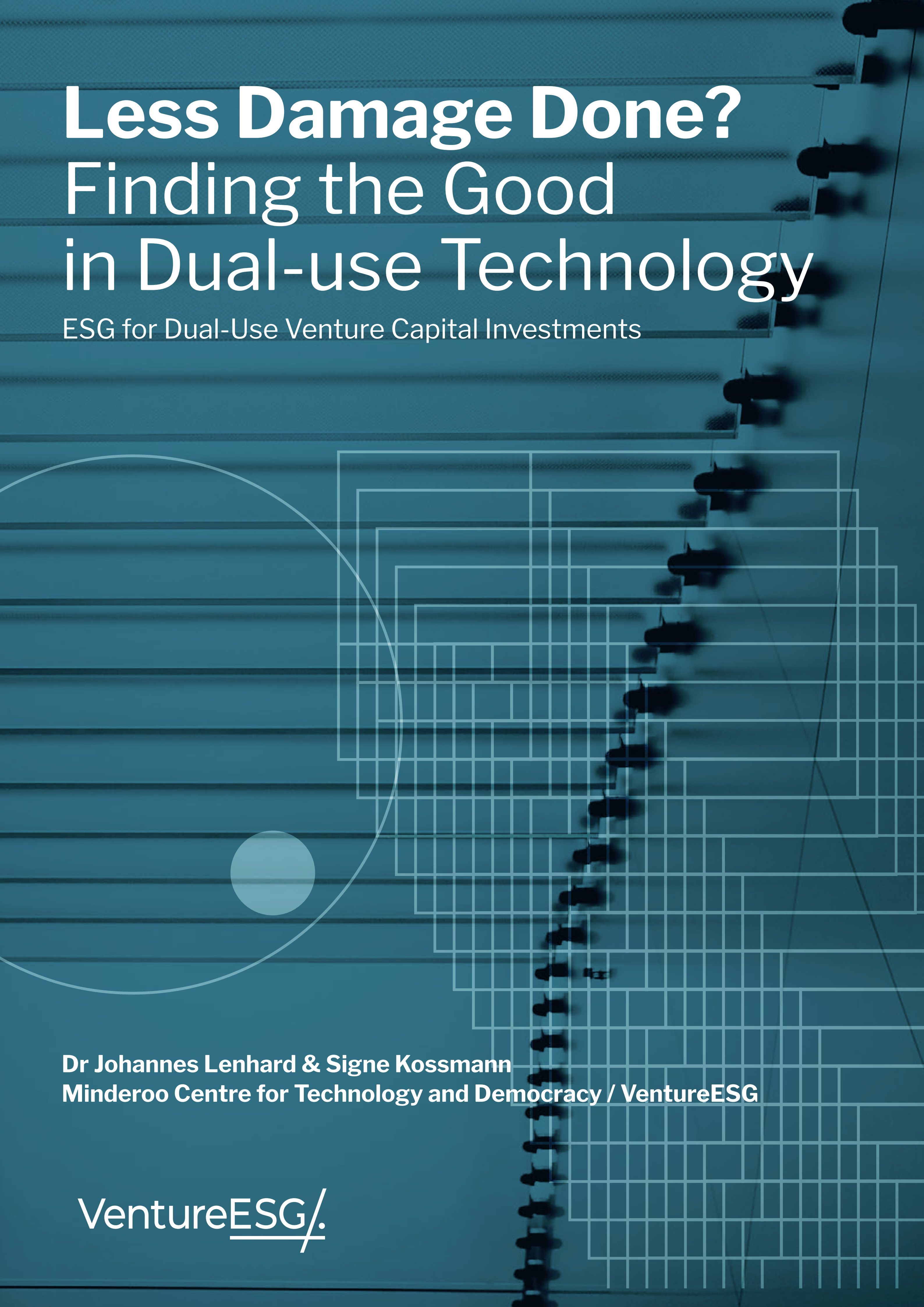


Less Damage Done? Finding the Good in Dual-use Technology

ESG for Dual-Use Venture Capital Investments

Dr Johannes Lenhard & Signe Kossmann
Minderoo Centre for Technology and Democracy / VentureESG

VentureESG

The Minderoo Centre for Technology and Democracy (MCTD) at the University of Cambridge.

VentureESG is a community-based non-profit initiative from VCs for VCs aiming to enable the integration of good ESG practices within the industry. We work with 500+ VC funds and 100+ limited partners and asset owners worldwide on meaningful ESG integration in VC. This project was led by our VentureESG Co-Founder and Co-Director, Dr. Johannes Lenhard with the dual-use research fellow Signe Kossmann. You can learn more about VentureESG here.

Funding and partnerships: the tool and white paper were generously funded by a grant from the ESRC Digital Good Network and housed at the University of Cambridge's MCTD in partnership with VentureESG. We also received guidance and feedback from Susan Winterberg (Research Fellow, VentureESG) Hannah Leach (Co-Director, VentureESG) and Prof Dame Fiona Murray (Dean of Innovation, MIT).

Note: The views expressed in this document are those of the authors and do not reflect the views of MCTD or the interviewees collectively.

Contents

Executive Summary

Recent geopolitical events – from the Russian invasion of Ukraine to the Israel-Palestine conflict – have led to rising European defence budgets, in some cases for the first time since World War II. Attitudes towards investing in defence and dual-use technologies have shifted in parallel. The role of venture capital (VC) funds and the early stage technology companies they invest in has seen a particular rise: an ecosystem that was mostly reluctant to fund defence and dual-use innovation, at least in Europe, has started to turn.

Given the nature of defence and dual-use technologies, i.e. innovation with both a civil and military application, and the novelty of the sector for VC investors, safeguarding is particularly critical. Existing tools which both investors and their limited partners (LPs) use - due diligence frameworks, exclusion lists – are often not fit for purpose for the sector. This research and the resulting white paper and tool aim to fill this gap.

Building on an exploratory research project and an initial white paper, we interviewed 33 VC investors, limited partners and ecosystem experts with exposure to dual-use startups between September 2023 and March 2024, across the UK, Europe and the US. Our conversations focused on current challenges with dual-use investments, especially from an ESG (environment, social governance) responsible investing perspective and with a strong focus on Europe.

We observed three common general challenges among our interviewees.

- A **lack of clear definitions** relating to 'dual-use' and 'defence' technologies stifles action, something that a more discretionary and engagement-focused approach might help overcome.
- Navigating existing **regulatory frameworks** proves challenging; often enforced regulation, such as exclusion lists, are not fit for purpose. Public-private dialogue could help.
- Lastly, dual-use technologies have unclear (and often under-explored) unintended consequence; fit-for-purpose ESG and impact frameworks and measurements are needed.

In addition, five ESG challenges specific to dual-use were surfaced by the investors and LPs we spoke to:

- Safe capital and customers: where money comes from and whom products are used by matters
- Human rights issues, especially in the dual-use supply chain (e.g. sourcing of rare earth materials)
- Environmental issues specific to dual-use technologies
- Data security issues, such as malign data use (e.g. cyber attacks and surveillance)
- Responsible product design principles to mitigate against unintended consequences

Based on our interviews, our earlier report and a survey of existing tools, we developed a sector-specific 'Universe of ESG Issues' . The tool is a first-of-its-kind due diligence framework for dual-use and deep tech and will support VCs and asset owners in embedding ESG into their decision-making and support early on when considering dual-use and defence tech companies.

1. What are dual-use technologies?

Defining and historizing dual-use

According to the EU, dual-use refers to “goods, software and technology that can be used for both civilian and military applications” (European Commission). Different definitions[1] reflect a lack of clarity, tensions and blurred lines about the difference between defensive or offensive capabilities, civilian or military applications, and peacetime or non-peacetime use (Michel, Q. et al 2020). These definitions permeate adjacent sectors to the defence sector, for instance the public and healthcare sectors. The confusion is partly created by the number of technologies which dual-use technologies include, from fields as diverse as biotechnology, satellites, artificial intelligence (AI), nanotechnology and quantum technologies.[2]

Dual-use technologies originated from R&D programs in military organizations and the US federal government, especially during the Cold War years. Given the Cold War context in which dual-use technologies originate, debates surrounding the transfer of defence technologies developed for military purposes into the civil realm have been central. In its primary definition, “dual-use denoted a civil application that might be derived from military research”, according to the Bulletin of Atomic Scientists. Today, both directions are common: dual-use technology is often describing a transfer from the civil sector, for instance, research on AI or biotechnology, to defence applications.

[1] Definitions vary, for an overview see: ‘Definitions of concepts: dual-use goods’ (in Michel, Q. et al (2020).
[2] For illustration, see a list of recently funded (European) defence and dual-use startups by Sifted here from 2024.

The spectrum ranges from civilian VCs (with very limited exposure to dual-use and defence) to a dual-use VC (with a vertical dedicated to defence) and a defence technology VC (whose sole mission is to invest in defence technology).

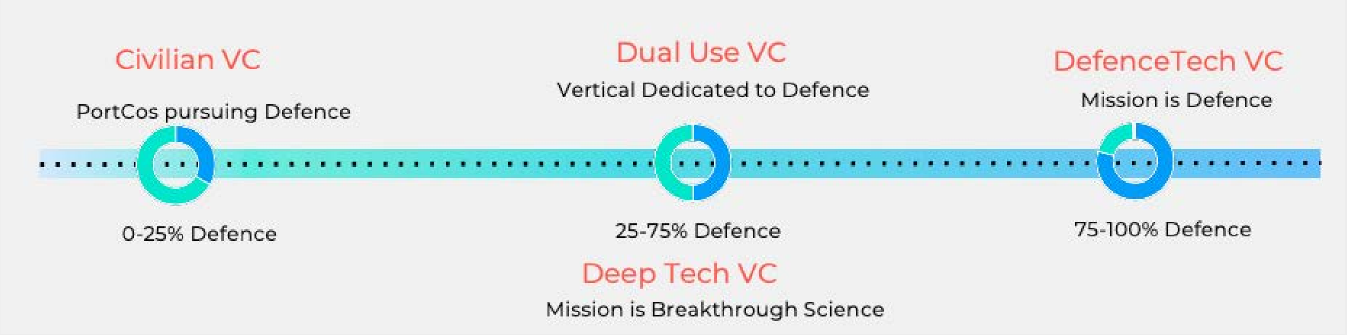


Figure 1: The Defence and Dual-use VC spectrum (VentureESG / Susan Winterberg)

Dual-use technologies have played an important role in scientific and technological advancement throughout the 20th century including, most famously, to develop the underlying technologies leading to the internet and iPhone including semiconductors, GPS, and battery and display technologies. Several key shifts have taken place in the development of dual-use technologies over recent decades.

Research and development in the US saw a rapid shift since the beginning of the Cold War from strictly government-led innovation towards what we now call public-private partnerships and defence innovation primarily developed in the private sector but funded by government grants. The Defence Advanced Research Project Agency [now ARPA], the R&D agency of the US Department of Defence, was a key player leading R&D in national security defence innovation in the US since its establishment in 1958 following the launch of then-Soviet Sputnik 1 satellite (Ueno 2023). While initially focused on space, with the launch of NASA in 1958, it soon focussed on computing, communications and biotechnology, one of its key dual-use developments being “ARPANET for military digital information sharing, a precursor to the Internet” (MassChallenge 2023).

For the golden years of venture capital and tech since the dot-com bubble burst in 2000, dual-use technology was at best in the background. During the 2000s and 2010s, venture capital investors focused mainly on consumer digital platforms (related to the rise of the internet first and then the smartphone), a Belfer Center report (2020) writes. During those years, European investors generally excluded dual-use from their portfolios. This is in contrast to the US, where, in 2022, American VCs still in 2022, American VCs invested more than $30 billion into defence tech start-ups compared to $2 billion in Europe.

In the EU, this historic reluctance has recently turned into a growing appetite for dual-use and defence innovation. Historically, defence spending went into expensive and slow-to-respond technologies (e.g. missiles) and not into cheap, fast-to-respond platforms (e.g. drones) leading to "critical gaps in Europe's defensive capabilities against current and future military aggressors", Jack Wang and Uwe Horstmann write. Minimal R&D spending by Europe's biggest defence companies led to a considerable lag.

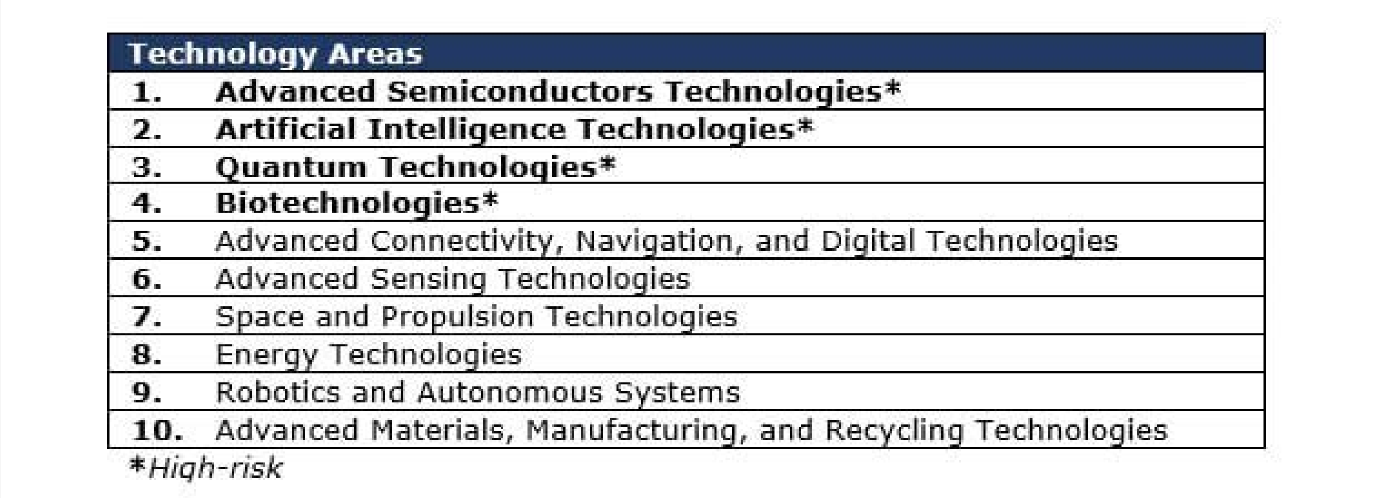
However, "Between 2013 and 2022, the total value of equity investment secured by UK defence tech companies rose from £15.4m to a record £295m", a report by Beauhurst and MD One reveals. Record highs are also seen in deal activity globally into defence and aerospace firms from private equity (PE) and VC investors: $20 billion in 2022, up from an average of $10.4billion, according to data from PitchBook for the Financial Times (Beauhurst / MD One).

In the past years, the defence technology sector has become a hotspot for VC investments; the Russian invasion in Ukraine highlighted the need for defence innovation leading to massive growth across, especially in cybersecurity, AI, space, and communications. A historical moment was defence tech startup, Anduril, raising $1.48 billion to modernize the US military's tech arsenal, supplying drones and AI software to the Ukrainian army. As Matthew Panzarino, former Editor-in-Chief at TechCrunch observed: *"Once an arena just for contrarian VCs, miltech [or defense tech] is booming and there is an appetite for the government sector to outsource R&D to the VC crowd".*

Similarly, in Europe, German AI startup Helsing raised several rounds of venture capital funding since it was founded in 2021, culminating in a €1.5 billion valuation last year. Helsing.ai became the first European defence technology unicorn and is now developing software using AI to rapidly process and analyze data from battlefields to support European militaries in their decision-making.

Changing attitudes to the defence sector in Europe has been seen in historical increases in defence spending in budgets, and shifts by institutional players, LPs and pension funds updating their investment approaches towards defence, ESG Investor reports. Swedish bank, SEB, reintroduced defence investments again, Sifted writes.

Most recently, we have also started to see political shifts in Europe around the framing of dual-use and defence technology. On October 3 2023, the European Commission unveiled a list of 10 critical technologies [see below] qualified as critical to EU economic security, of which four (semiconductors, AI, quantum technologies and biotechnologies) are most likely to affect EU technology security and technology leakage. Analysts at the European Council on Foreign Relations argue that this signals a key shift in the EU to de-risk away from a conservative technology strategy, yet that there is far to go.



Technology Areas	
1.	**Advanced Semiconductors Technologies***
2.	**Artificial Intelligence Technologies***
3.	**Quantum Technologies***
4.	**Biotechnologies***
5.	Advanced Connectivity, Navigation, and Digital Technologies
6.	Advanced Sensing Technologies
7.	Space and Propulsion Technologies
8.	Energy Technologies
9.	Robotics and Autonomous Systems
10.	Advanced Materials, Manufacturing, and Recycling Technologies

**High-risk*

Figure 2: Critical Technology Areas for the EU's Economic Security (Dow Jones)

Most of the critical technologies in the European Commission's list are squarely in the focus for VC investors, bringing about, as one commentator argued, a 'new era of defense readiness' both in Europe and – with a longer history – the US. Now that dual-use tech has arrived on the European agenda for both policy makers and (VC) investors, what are the challenges with safeguarding these investments and technologies?

Regulating dual-use

Dual-use items are highly regulated in the EU in terms of their export, transit and transfer. On 15 September 2023, the European Commission updated its EU Control List of Dual-Use Items [see below] - what it considers dual-use and are therefore regulated, to include further particularly sensitive items manufacturing equipment of high-performance computers and lasers, and propulsion motors for submersible vehicles. In the UK/EU, dual-use items include physical goods, software and technology and are set out in 10 categories, with five sub-categories each.

0 = Nuclear materials, facilities, and equipment	A = Systems, equipment, and components
1 = Special materials and related equipment	B = Test, inspection, and production equipment
2 = Materials processing	C = Materials
3 = Electronics	D = Software
4 = Computers	E = Technology
5 = Telecommunications and information security	
6 = Sensors and lasers	
7 = Navigation and avionics	
8 = Marine	
9 = Aerospace and propulsion	

Figure 3: EU Control List of Dual-Use Items

European regulation is framed such that dual-use and defence "can contribute to international peace and security and prevent the proliferation of Weapons of Mass Destruction". Generally, governments establish regulations and control measures to prevent the illicit or societally harmful use and development of dual-use technologies, for instance, by monitoring and managing their transfer, also known as 'dual-use technology transfer.[3]

There are a variety of other regulations for dual-use technologies, mostly focused on export controls:

- *National:* The US has the most comprehensive export control laws [U.S. Export Control Reform Act of 2018], while the UK regulates dual-use technologies through the UK Strategic Export Controls List.
- *International*: International treaties oblige member states to consider the control and export of goods and technologies capable of being Weapons of Mass Destruction [Chemical Weapons Convention; Treaty on the Non-Proliferation of Nuclear Weapons, Biological Weapons Convention] as well as multilateral export control regimes, such as the Missile Technology Control Regime, which aims to coordinate national export licensing agreements on unmanned delivery systems.

How does ESG relate to dual-use?

ESG is becoming a key priority in the defence industry and is already receiving significant investor attention according to a report by Army Technology. However, the understanding of (material) ESG for dual-use and defence startups is underdeveloped for VC funds. As we found both in our earlier report and interviews for this research, VC investors who are exposed to dual-use and defence tech mostly lack comprehensive frameworks and guidelines.

This is despite the existence of very strong rationales for safeguarding and clear responsible investing principles. Tensions specific to dual-use and defence tech involve, among others:

- *Surveillance and privacy concerns:* dual-use surveillance technologies, such as facial recognition systems and social media monitoring tools, are increasingly being used and can infringe on privacy rights, leading to profiling and racial discrimination, or be used for spyware (see Renew Europe on cyber surveillance).
- *Lethal Autonomous Weapons Systems (LAWS)*: AI can be used to develop LAWSs and military AI, which raise human rights concerns, a report by SIPRI explores, by violating International Humanitarian Law (IHL), in targeting civilians, being indiscriminate or causing disproportionate harm. The International Committee of the Red Cross (ICRC) warns that the removal of *meaningful* human control

[3] The EU defines 'dual-use transfer' as "the ability to adapt a technology developed in one sector (defence or civil) for use in the other (civil or defence)".

over weapons systems can also lead to significant adverse civilian impacts (see BBC on AI's role in defence tech).

- *Cybersecurity and data protection:* cybersecurity technologies with dual-use potential can infringe on data protection and digital rights, as well as the risk of technologies being used for cyber attacks or hacks. Most recently, The Financial Times reported a breach of the records held by a Ministry of Defence contrary's IT system of UK military personnel in a cyber attack allegedly by China (see FT covering suspected Chinese cyber-attacks on UK's MoD).
- *Concerns around environmental footprint of supply chains*: another critical ESG issue relates to supply chains and transport involved in developing dual-use and deeptech. Semiconductor and chip manufacturing tends to rely on complex cross-border supply chains to source parts that have very high environmental impact, using great quantities of water and energy and leading to hazardous waste (see Science Direct on the chip industry's environmental impacts)
- *Quantum computing and concerns on cybersecurity*: given their ability to radically upend existing encryption practices, there is great concern that quantum computers will be used for hacking, and if used in the Healthcare and Life Sciences sector for gene-editing, there are issues around data harvesting (see Wall Street Journal's coverage of quantum's ethical risks)

Given the potential adverse uses of digital dual-use technologies, and the digitization of conflict, for instance, cyber warfare in conflict situations or the use of military AI to enhance the lethality of weapons, the ICRC has developed guiding principles in a 2023 report to mitigate against these developments and protect civilians.

Other existing responsible investment standards – e.g. UNPRI VC guidance, SASB/ISSB materiality assessments, MNE guidance or the ILPA DDQ for LPs – are not tailored to the needs and challenges of VCs and early-stage technology companies in general, and dual-use and defence tech in particular. But with the general push for more integration of ESG across sectors and ecosystems, ESG has started to be applied to the defence sector: "The UK defence sector has embraced ESG considerations', Andrew Griffith and Defence Minister James Cartlidge proposed recently in a UK Ministry of Defence Joint Opinion Piece on ESG (2023). The EU Taxonomy Minimum Safeguards discuss exposure to controversial weapons. The translation of ESG into early stage tech and startups, funded by VC investors, is still lacking, however. The question and task remains: how can VC funds embed ESG into their decision-making and support *early on* when considering dual-use and defence tech companies?

2.

Key general challenges and solutions

Our interviews surfaced some general challenges VC investors in the dual-use and defence tech sectors encountered, from the aforementioned lack of clear definition and general transparency to lagging-behind regulation and the lack of a fit-for-purpose impact framework. In this section, we provide more detail on the most common challenges and propose solutions and next steps for these particular challenges.

2.1 Lack of clear definitions stifles action

VCs and LPs we interviewed shared concerns about the lack of consistency and clarity concerning definitions and terminology relating to 'dual-use' and 'defence'. Many, especially in the US, avoided using the term 'dual-use' because of such confusion. One VC reflected the broader dilemma of the lack of transparency about whether a certain product or service was being sourced and used in a military context, partly worsened by barriers posed by national security, classification and confidentiality.[4] VCs who are only now starting to invest in dual-use technologies take definitions - beyond regulation – even more lightly, judging from the conversation with one European VC in particular:

> *"Dual-use technologies can be anything, it's in the eye of the beholder." [European VC].*

[4] In our earlier research (available here), we found that nuances in language and a lack of clarity led to confusion by investors, e.g. differences in understandings of offensive versus defensive use of weapons led to misunderstanding on what are allowable investments: an exclusion list may list a technology with offensive capabilities, but "often the same technology could be used in both offensive and defensive applications."

Often terminology and definitions used are in fact too broad; standard exclusion lists used by LPs – e.g. from the European Investment Bank (EIB) or the International Finance Corporation (IFC) – exclude VCs from investing in 'weapons' but are not specific enough to differentiate between different dual-use technologies.

When it comes to ESG for dual-use, most interviewees cited the lack of standardized mechanisms for KPI and data reporting, for instance. Beyond certain LP reporting templates (e.g. Invest Europe template), there is still a general lack of independent assessment or reporting for ESG in VC.[5] Generic ESG metrics do not easily map across companies and must be tailored to a company's sector (i.e. materially filtered); for dual-use, no specific ESG criteria are available.

Proposal: towards a discretionary approach and early engagement

Our interviewees proposed that having a very strict definition is not necessarily going to solve this challenge. Instead, considering dual-use more broadly in terms of a technology's potential and exposure to military application might be more useful. For instance, in due diligence, the investor's focus should first of all be on the founder's intentionality, and consider intended and unintended applications of the technology. Side letters can help enforce particularly strong exclusions (e.g. of customers in certain geographies).

Additionally, formal exclusion lists need to be rethought, especially for European LPs. They can undermine security, CEPA analyst writes. However, Devex reports that, as part of the European Commission's new defence industrial strategy, the EIB is looking to "adapt defence-related exclusions" and is urged to "support production of military equipment and more generally the European defence industry". In April 2024, the EIB updated its dual-use definition loosening its restrictions on investment in technologies with civilian and military applications: "Going forward, the Bank will waive the requirement that dual-use projects derive more than 50% of their expected revenues from civilian use". This signals its commitment to security "while maintaining the highest ESG standards", the Bank writes. Attempts to a nuanced exclusion list include the Church of England's Ethical Investment Group's rejection of the blanket exclusion of defence companies; they allow investment into 'military IT and software' and will have a conventional weapons exclusion for companies with 10%+ turnover from 'strategic military sales'.

Given the continuing lack of clarity, there are two possible approaches for LPs and VCs: open dialogue and ongoing engagement. Dialogue, e.g. as part of making an investment decision, between the LP and the VC can help define red lines on what is in and out of scope case-by-case. We heard from one LP that they prefer this approach of continuous communication.

Engagement between the VC and company post-investment can also help to create more trust and transparency. For many of our VC interviewees a 'pragmatic approach' around intentionality of founders was a first step in DD which can translate into active stakeholder management. A strong strategy is proactively engaging portfolio companies with a 12-month 'impact plan' with ESG actions and regular check-ins (according to an EU-based deep-tech VC).

2.2 Regulation needs to be updated - industry dialogue can help

Conducting due diligence on a dual-use tech company can be challenging due to limited transparency and confusing regulatory requirements. Navigating regulatory frameworks poses a challenge for startups with limited capacity and VC investors. While export control regulations of defence tech, like the EU's, are robust and clear, dual-use regulations are recent paradigms, one LP said; the result is the continuously shifting scope of these regulations. As recently as October 2023, the EU introduced controls on autonomous items. Regulation needs to be updated, Amnesty International reports, for instance by placing new forms of digital surveillance items on the dual-use control list, like biometrics.

Challenges also arise in having to consider cross border regulations due to complex global supply chains of dual-use technologies, e.g. for transport routes, each country has a dedicated dual-use list, which tends to differ between country of origin, destination and even a third country [UK, LP]. This requires additional constant monitoring of changing regulatory landscapes, where public-private dialogue would be helpful. In the US, ITAR was written before software developments and is out of pace with digital

[5] This is despite the standardized European regulation (Sustainable Finance Disclosure Regulation, SFDR) which many VCs have to report on. This regulation is in itself not materially filtered or fit-for-purpose for VC, however.

innovation, while for data protection, regulation can be confusing: "In the US, we would ask if the company is FedRAMP certified and to what level. I'm not sure if there is a European equivalent", one interviewee shares [Ecosystem expert, US].

In light of this, VCs are proactively engaging governments. To start the dialogue towards updated regulation, in the US, 13 tech executives and VCs wrote an open letter to Defence Secretary Lloyd Austin drawing on recommendations from the Atlantic Council's Commission on Defense Innovation Adoption in 2022. They were calling for an improved Defence Innovation Unit and to scale up new technologies: "Antiquated methods [...] have drastically limited the Department of Defence's [...] access to the best commercial innovation. This must change."

Proposal: a public-private dialogue

Governments can draw on the knowledge and expertise of VCs (and their portfolio companies) in the dual-use sector to produce regulations and legislation that is more evidence-based and fit-for-purpose. As part of this, developing positive use cases can help shift the narrative of defence technology and innovation, for instance, their use in peace and security contexts, from increasing public safety, such as preventing terrorism and protecting military personnel by enhancing battlefield safety. Many positive environmental cases exist, too. "Quantum computing will likely transform the fight against climate change", Deloitte reports, by optimizing resource consumption, making supply chains and electric grids more efficient, while radically reducing carbon emissions.

Public-facing support can go a long way to shifting these narratives: most recently, UK Prime Minister Rishi Sunak said: "Investing in defence companies contributes to our national security, defending the civil liberties we all enjoy", The Times writes. In terms of specific ESG regulation, we don't expect regulators to adapt existing regimes (e.g. SFDR) to the requirements of venture capital and early stage technology companies; we are even less confident that regulation will ever steer away from a standardized approach focused on reporting. The key drivers of rules (and quasi-regulation) in any given sector or ecosystem are hence the limited partners and asset owners who are increasingly engaged in dialogue (see 2.1).

2.3 Unclear unintended consequences - dual-use between public good and danger

An investment in AI could fuel the development of AWS or surveillance technologies, while quantum technologies could be used for medical imaging and diagnostics or hacking. The application of dual-use technologies – often related to years-long university research – are endless and similarly ambiguous. This is termed the 'dual-use dilemma', in which scientific and technological research is intended for good, but can also, either intentionally or accidentally, be used for harm", Amy Webb, professor of strategic foresight at New York's University's Stern School of Business writes for the Atlantic, on the next pandemic stemming from biowarfare.

The most prolific example of an unintended consequence: the scientific discovery of ammonia transformed agriculture, yet was a fore-runner to the creation of chemical weapons. This has led to treaties such as the Chemical Weapons Convention to limit harms from research. Yet, while the Biological Weapons Convention prohibits the development, production and stockpiling of weapons, research for defensive purposes is possible, Dr Lentzos writes for the Nuffield Council on Bioethics and biological research can be misused to pose a biologic threat to public health and/or national security.

Today, the lack of maturity of many dual-use technologies makes it difficult to know what their potential future uses and impacts will be. The separation between the development of individual parts and how they are used makes oversight of their consequences challenging. Unintended and intended consequences – as with any startup technology – are unclear and so are the technology's impacts. Many of the investors we interviewed in fact consider themselves to be advancing the public good, but are concerned they are viewed as unethical in the public eye.

"Defence has an ethical and fundamental role in society, and by excluding it, [LPs] are actually risking the future stability and foundation of society" [Dual-use VC, US].

Unsurprisingly, the sentiment of VC investors who are investing in dual-use echoes the sentiment by William Hague in 2023, "the attitude that the defence of a free society is an unethical activity must be abandoned". VCs furthered observed taboos related to the defence industry, mostly based on a lack of awareness and public-facing visibility. For some, investing in dual-use technologies with military applications still carries a risk of reputational damage, including when it comes to the attraction and retention of employees.

Proposal: more responsible product design and impact measurement

In the dual-use space, frameworks to enhance responsible product design, specifically on unintended consequences and the measurement of impact are lacking but desperately needed. Despite its contribution, defence is largely omitted or excluded as a category of 'impact investment', our earlier research found, or does not fit into existing impact metrics (Winterberg et al. 2020). A first step could be to include more ESG issues when making investment decisions (see below), with a focus on material issues at the product development stage, while considering the case and sector-specific unintended risks. Fit-for-purpose impact metrics could be a second step. Some potential practices include:

- *Material deep dives*: addressing the materiality of emerging technologies through detailed assessments of capabilities, use cases and mitigations
- *Forecasting and proofing*: for instance through 'causality chains' (Winterberg et al. 2020)
- *Integrating direct and indirect/spillover effects*, asking questions like[6]:
  - » "Who else might want to use the product?"
  - » "What new scientific discoveries could advance the capabilities of our product?"
  - » "With which other technologies could our product interface?"
- *Simulations and exercises*: to stress-test designs
- *Impact measurement*: with metrics that articulate how defence technology provides ESG benefits: preventing terrorism, conflicts, cyber attacks, damage to critical infrastructure; protecting democracy, freedoms and the rule of law.

[6] The following questions are from Winterberg et al. (2020), Responsible Investing in Tech and Venture Capital Advancing Public Purpose in Frontier Technology Companies. Cambridge MA: Belfer Center, Harvard Kennedy School.

3. Key dual-use specific ESG challenges

In addition to the general challenges of VC investors in dual-use (Section 2), we also encountered ESG concerns and issues specific to dual-use. In this section, we discuss five of the most common issues.

3.1 Safe capital and customers

VCs investing in dual-use technologies emphasized significant regulatory barriers given sensitivities of the uptake of dual-use technology in a tense geopolitical climate. Specific political scrutiny beyond regulation occurs with regards to both the side of capital and the related (company and tech) ownership and unintended use by malign customers and users. This is part of wider trends in the "weaponization of capital" the FCC reports, as some state actors use private equity and VCs to gain access to critical technologies and IP. Concerns around capital flows, especially of private market capital, for instance from the US to the China, are particularly concerning:

> "Venture capital investments provide a licit path to technology and innovation. In some cases, venture capital investments might allow Beijing direct access to intellectual property. In other, more indirect cases, aggregated information about cutting-edge research and commercialization could be used to inform and direct Beijing's R&D bets" (FCC 2022).

We encountered many VC investors concerned about potential (or existing) co-investors, i.e. sources of capital for the dual-use tech companies. In particular, the (rising) tensions between US and Chinese interests resulted in concerns among US investors. The source of capital also potentially has an impact on intellectual property (e.g. who owns the company's IP?). Two US VCs shared their concern about where capital is from, which is particularly tenuous regarding digital defence technologies, which can be used for surveillance and in conflict contexts.

On the other side, VCs also face challenges beyond export regulations when it comes to users and customers of a technology. Regulatory and (VC-)desired restrictions are at times ambiguous and differ according to national, regional and international jurisdiction, which is especially complex when considering the international supply chains and customer base of a dual-use technology. Situations of adversarial capital that require extra scrutiny are laid out in President Biden's Executive Order to the Committee on Foreign Investment in the US, GreenbergTraurig writes, one being risks to cyber security: "to consider whether the foreign investor (including its relevant third-party ties) may as a result of the investment directly or indirectly obtain the ability to harm U.S. cybersecurity' or could extract sensitive data."

3.2 Human right issues in the dual-use supply chain

There are significant challenges related to the often complex and cross-border supply chains for hardware tech companies, which many dual-use companies are. As dual-use and deeptech tend to rely on parts, for instance in the production of microchips, VCs are concerned about a variety of potential issues. Bottlenecks in procuring supplies, supply chain disruptions (e.g. for materials coming from conflict-ridden countries such as the DRC or regulatory changes influencing supply chains such as further export controls on materials. Not only did interviewees refer to a lot of unknown variables, a lack of oversight of the trans-national supply chain furthermore translated into difficulties of monitoring procurement practices, and ensuring traceability and accountability throughout the supply chain. Of special importance are potential human rights-related issues in the supply chain. For instance, sourcing rare earth minerals (used for microchips) associated with poor labour conditions, including child labour (Amnesty International), and issues around land use negatively affecting local populations, for instance, by mining in areas affecting Indigenous territories (IPS).

A way forward is enhanced human rights due diligence, as "traditional E&S due diligence may not use international human rights standards", BII writes. VCs can also endorse principles, such as OHCHR's Guiding Principles on Business and Human Rights, which require not only assessing risks along the supply chain, but also integrating findings, tracking responses and communicating them. Companies are also being asked to disclose human rights risks: "The UK Modern Slavery Act, the California Supply Chain Transparency Act, and the US Federal Acquisition Regulations all require companies to explain the steps they have taken to ensure they are not connected to slavery or forced labour in their value chains", BII reports.

3.3 Dual-use specific environmental issues

Digital dual-use technologies – from space tech to quantum – tend to rely on raw materials, such as rare earth metals and minerals, such as lithium, cobalt and nickel. These extractive processes pose environmental risks, for instance polluting underground water, soil and land at the largest global REE extraction and processing site in Bayan Obo, China (IPS). Semiconductor production is known to involve extensive water and energy use (ScienceDirect): the semiconductor foundry, "TSMS, alone uses almost 5% of all of Taiwan's electricity", the Guardian reports. Electronics manufacturing contributes to hazardous waste that includes pollutants like heavy metals and corrosive materials (Veolia). Additionally, many digital dual-use technologies rely on AI technologies which in turn rely on large quantities of data and using algorithmic computing. The energy intensity (and carbon footprint) of cloud storage and AI-models, for instance for cooling data centers, is increasingly seen as a critical problem of tech companies, especially as they scale (Yale).

3.4 Malign use of data, violations of data security and wider human rights issues

Malign use of data for targeted or mass surveillance, spyware and hacking is growing and unjustly used for profiling ethnic and racial minorities, while 'algorithmic discrimination' is systematically reinforcing inequalities, a BSR report finds.

In the dual-use space, issues of data security relate to wider human rights, for instance, infringements by surveillance technology providers and private military companies, a report by Privacy International and the Geneva Centre for Security Sector Governance finds. Surveillance using biometric features, e.g. facial recognition, is especially concerning and reveals wider questions of digital rights and privacy. While mass surveillance technologies were recently banned in the EU AI Act, "It [...] fell short of upholding human rights when AI systems affect migrants, refugees and asylum seekers", Amnesty International reports.

Violations of data security are prime in cyber attacks: not only do they try to steal data, but they also seek to control systems critical to the functioning of society (Allianz). Cyber attacks on critical infrastructure, like hospitals and dams, or targeting power grid's, such as in Ukraine in 2022 (Reuters) and hacks of the UK's Sellafield nuclear site (The Guardian) pose existential threats to public safety.

Moving forward, improving responsible product design to secure data systems could entail asking whether the development of software adheres to security protocols, such as the UK National Cyber Security Centre's 'secure by design' principles, while Privacy International has proposed a safeguarding framework for security providers to mitigate data breaches.

To mitigate issues of bias in digital technologies, one US VC also said: “We need more participation”,for instance, through the inclusion of underrepresented groups in training data and board representation.

3.5 More responsible product design principles can help with unintended consequences

Responsible innovation (RI), according to the UKRI, “aims to ensure that unintended negative impacts are avoided, [...] and that the positive societal and economic benefits of research and innovation are fully realized”.[7] Equitable adoption and diffusion is part of this, with exemplary initiatives like Citizens Forum on AI and automated decision-making and a public dialogue on quantum technologies. The first UK funding body to incorporate RI principles was the UK's innovation agency (Tait, et al. 2021), while headway is being made on responsible product design in domains like AI and digital product development. But, much is to be done, and several VCs mentioned questions around responsibility limiting their role.

> *“Legally, [our responsibility] stops after exit, but as responsible investors, we are concerned” (LP, UK).*

[7] Other standards include th British Standards Institutions Responsible Innovation (RI) guide

When focusing in particular on AI technologies and autonomous components (e.g. for drones), introducing principles of responsibility in the development and application phase of the technology is quickly becoming best practice. Especially a focus on 'human-in-the-loop' has been raised repeatedly by our interviewees when discussing autonomous systems.

Designing principles needs public sector engagement. Moves by governments to design ethics into AI in defence, to a first ever summit on the “responsible” use of military AI is paving the way. “We're taking the first step in articulating and working toward what responsible use of AI in the military will be“ says the Foreign Minister of the Netherlands in Reuters. Other principles include NATO's Principles of Responsible Use of AI in Defence, specifically produced for the defense section[8]:

Lawfulness:	AI applications will be developed and used in accordance with national and international law, including international humanitarian law and human rights law, as applicable.
Responsibility and Accountability:	AI applications will be developed and used with appropriate levels of judgment and care; clear human responsibility shall apply in order to ensure accountability.
Explainability and Traceability:	AI applications will be appropriately understandable and transparent, including through the use of review methodologies, sources, and procedures. This includes verification, assessment and validation mechanisms at either a NATO and/or national level.
Reliability:	AI applications will have explicit, well-defined use cases. The safety, security, and robustness of such capabilities will be subject to testing and assurance within those use cases across their entire life cycle, including through established NATO and/or national certification procedures.
Governability:	AI applications will be developed and used according to their intended functions and will allow for: appropriate human-machine interaction; the ability to detect and avoid unintended consequences; and the ability to take steps, such as disengagement or deactivation of systems, when such systems demonstrate unintended behaviour
Bias Mitigation:	Proactive steps will be taken to minimise any unintended bias in the development and use of AI applications and in data sets

Figure 4: NATO's Principles of Responsible Use of AI in Defence (NATO)

[8] In an earlier piece of work at VentureESG we partner with Ravit Dotan to produce a specific due diligence framework for any AI company (not specific to dual-use); you can find that here.

4.

Next steps: towards a fit-for-purpose due diligence tool

What our research and conversations with investors and asset owners clearly showed is the lack of specific ESG tools. Starting with an approach to enhance investment decision making, our focus in the second part of this project was on the development of a list of specific questions, helping investors to uncover potential ESG risks. The result is our ‘Universe of ESG issues for dual-use and defence tech companies’.

Dual-use specific ‘Universe of Issues’ for due diligence

As with all our due diligence tools (e.g. for biotech or crypto), this ‘universe of issues’ is primarily a tool for venture capital investors to practically guide their due diligence and investment decision making. We compiled circa 70 sector-specific questions for VCs to scrutinse dual-use and defence tech companies in different sectors and different levels of maturity.

You can find the open-access framework here and by clicking the below button.

Due Diligence Tool

Next steps

A due diligence tool can certainly only be the first step towards helping VC investors (and LPs) make better investment decisions. Similar tools, e.g. industry specific materiality assessments or a specific LP DDQ as well as frameworks to support dual-use portfolio companies post-investment are needed.

This research and tool are hence only the first steps in our journey to collaborate with VCs and LPs in the dual-use sector. We are running a working group specific to the topic at VentureESG (please email hello@ventureesg.com if you are interested in joining) and are keen to receive any feedback you might have.

05. Appendix

I: Methodology

We developed this research in close collaboration with the VC ecosystem to meet their needs and reflect material priorities. Between October 2023 and May 2024, we rolled out four phases for the research. They included:

Phase 1:

Horizon-scanning and desk research. This aimed to lay out the landscape of ESG concerns specific to dual-use technologies.

Phase 2:

Preliminary interviews with ESG community to define key issues.

Phase 3:

Semi-structured interviews with sector-specialist VC investors to identify the prior ESG issues and DD guidance. We interviewed 33 VC investors, limited partners and ecosystem experts with exposure to dual-use startups between September 2023 and March 2024, across the UK, Europe and the US. We mainly engaged the VentureESG network and contacts through a 'snowball' method. Formal interviews and informal conversations enabled us to 'glean the everyday meanings [and] tacit assumptions' (Lichterman 2002). A reflexive and pluralistic approach to our methods meant that we held several cycles of data collection and analysing our findings to constantly adapt our DD framework.

Phase 4:

Workshops and tool development. We shared an initial version of the DD framework within the VC and asset owner industry. We subsequently shared the tool with all interviewees to stress-test our findings and receive feedback to nuance the framework in a reflexive manner.