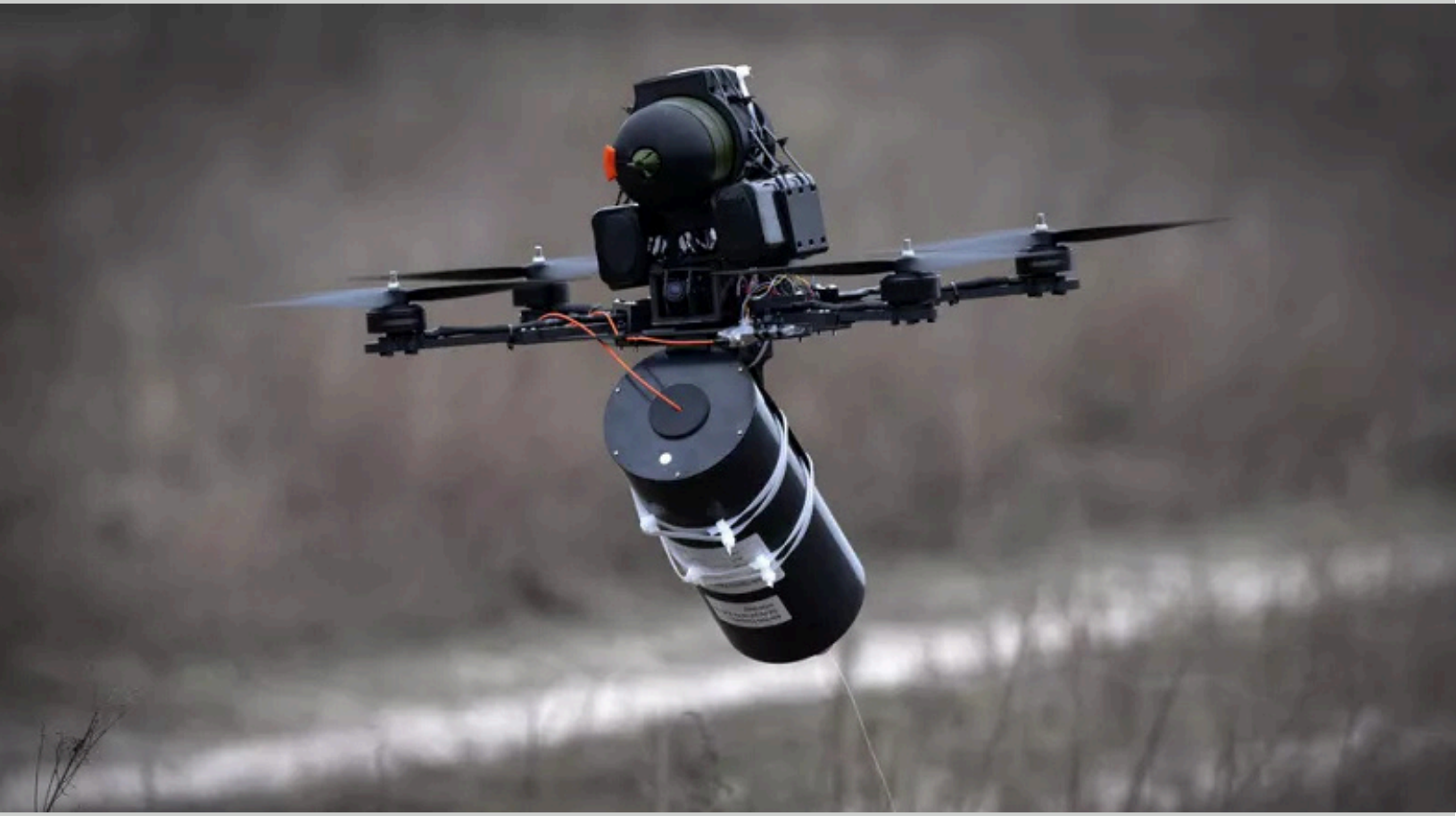
Cornell Brooks Public Policy

Tech Policy Institute

Who Draws the Line on Dual-Use Defense Technology?



Sumajja Denysiuk

Who Draws the Line on Dual-Use Defense Technology?

Sumajja Denysiuk

There is a line somewhere between a commercial drone and an Unmanned Combat Aerial Vehicle (UCAV), between a data analytics platform and a targeting system, between satellite internet and military communications infrastructure. The question is not whether that line exists embedded in export control regimes, procurement rules, and legal definitions, but who drew it, how it evolved, and who benefits from keeping it where it is? That question matters because the line is doing national security work. When a government classifies a technology as military, it restricts who can build it, sell it, and export it. When it classifies that same technology as commercial, those restrictions fall away. The difference determines whether a rival state can acquire, through an ordinary commercial transaction, the same AI-enabled targeting tools that took allied defense establishments decades and billions to develop. A well-functioning classification system slows that diffusion and preserves the technological edge that underwrites deterrence. When it does not work, the erosion is quiet, incremental, and by the time it is visible, largely irreversible.

During the Cold War, that line was easier to police because the state occupied the center of the innovation system. Defense agencies funded much of the foundational research, military contractors operated inside a relatively closed industrial base, and export controls governed technologies whose strategic use was often visible at the point of production. The government was not simply trying to regulate the spread of technology after the fact; it had helped define, fund, and direct the technologies in the first place. The modern dual-use problem emerged as that relationship inverted: commercial firms now build many of the capabilities militaries later seek to adopt, while the state is left trying to classify technologies it no longer fully controls.

The system is not working, and the reason is not primarily technical. It is an accountability problem. Companies are encouraged to classify their own products; regulatory authority is split between the State Department and the Commerce Department, two agencies with overlapping and conflicting mandates; and the primary international regime runs on non-binding consensus any single member can veto. Responsibility for deciding what requires oversight belongs to no one in particular. The result is a system quietly captured by private actors with strong financial incentives to minimize oversight, subordinating national security logic to commercial incentives.

The foundational problem is definitional. The U.S. Department of Defense acknowledges that most modern technologies can qualify as dual-use, rendering the category functionally meaningless. In practice, policymakers mean something narrower: technologies developed for commercial markets and later adapted for military purposes. That distinction reflects a structural shift the classification system has not absorbed. The Department of Defense accounted for over 60% of total U.S. research and development spending during the Cold War. Today it accounts for less than 10%. The classification system remains rooted in a model where the government led innovation, not one where it is a secondary customer trying to regulate an ecosystem it no longer controls.

At the international level, the Wassenaar Arrangement was created to coordinate export controls among 42 nations on conventional weapons and dual-use goods. The logic was straightforward: if the participating states agreed on which technologies belonged on controlled lists and to whom they should not be sold, they could limit destabilizing transfers to adversaries and non-state actors. In practice, however, the arrangement operates by consensus, allowing any single member to block updates, delay new controls, or weaken proposed restrictions. Since it has no enforcement authority when members disagree, sensitive technologies can still diffuse to actors the regime was designed to constrain.

Domestically, the divide between the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) compounds the problem. The State Department regulates military-specific items under ITAR; the Commerce Department governs dual-use technologies under the more permissive EAR. The boundary is not fixed; it is negotiated, often by the companies themselves. Self-classification is the default. The Directorate of Defense Trade Controls can issue formal 'Commodity Jurisdiction' determinations and the Bureau of Industry and Security conducts enforcement, so self-classification is not the final word. However, because ITAR compliance can run into the millions annually, and since showing a product to a foreign employee on U.S. soil can constitute a deemed export requiring State Department authorization, the decision of which regime to classify under does not sit with engineers. It sits with lawyers and investors. The firms being regulated are also shaping the regulatory outcome.

The consequences cut both ways. In 2024, TE Connectivity paid $5.8 million in civil penalties for shipping ordinary-looking connectors to Chinese entities linked to hypersonic and drone programs. The parts were unremarkable; the end-users were not. Conversely, a 2025 State Department Rule moved an entire category of unmanned underwater vehicles into a less restrictive regime overnight worth more to affected firms than any lobbying campaign. The line is redrawn constantly by government actors as much as by companies gaming the system. Everyone who depends on it is standing on shifting ground.

That shifting ground has produced a distinct corporate strategy. Firms adopt a commercial-first approach, building products for civilian markets and adapting them for defence later. For startups, this is rational: defence procurement is slow and difficult to navigate, while commercial markets offer faster feedback and more accessible capital. For investors, dual-use companies offer exposure to both commercial growth and government contracts within a single bet. The label 'dual-use' is not just a regulatory category. It is a pitch deck slide.

The strategic consequence goes largely undiscussed. When the military becomes a secondary customer, it receives capabilities that lag behind the technological frontier, sometimes by years. In a competition defined by speed, that delay creates a structural disadvantage for countries whose adversaries integrate military requirements from the outset rather than retrofitting them later.

China's civil-military fusion (MCF) strategy illustrates what a deliberate alternative looks like. Rather than allowing the boundary between commercial and military technology to emerge organically, MCF seeks to collapse it by design: embedding military requirements

directly into civilian R&D funding criteria, requiring private firms to make intellectual property and data available to the People's Liberation Army on demand, and using state-owned enterprises as conduits to pull commercial technology into defense programs. Beijing has committed over $68 billion in dedicated MCF investment funds since 2015.

Implementation has been uneven. Persistent barriers between state-owned conglomerates and private firms mean that only around 2% of China's private high-tech enterprises were estimated to be involved in defense work as of 2019. China has not solved the integration problem.

But the structural difference in intent has a concrete implication: China is attempting, through centralized coordination and sustained political will, to compress the timeline between commercial innovation and military deployment. The United States is managing the same challenge through fragmented regulation, decentralized decision-making, and a classification system whose default is industry self-assessment. The asymmetry is not one of current capability. It is one of institutional seriousness and, over time, institutional seriousness compounds.

Nowhere is the classification failure more acute than in artificial intelligence. A model trained to identify tumors in medical imaging can, with relatively minor adjustments, identify targets in satellite imagery. A logistics optimization algorithm can coordinate supply chains or manage drone swarms. The underlying capability is the same; only the application changes, and that change can happen after export, after deployment, after any classification decision has already been made.

Export control regimes were designed for discrete, tangible goods. AI does not fit that framework. It is general-purpose, adaptable, and developed primarily by firms - among them Amazon Web Services, Google, Microsoft, and OpenAI, whose accountability is to shareholders, not national security agencies. The Pentagon seeks to deploy these models, but they were not built to military requirements and were not classified at the point of creation. Regulation has become reactive, attempting to govern capabilities after they have already diffused.

The confusion over where the dual-use line falls is the predictable output of a system where no single actor is responsible for drawing it. When classification boundaries are set by actors with financial incentives to draw them permissively, and the international architecture for challenging those decisions is non-binding and unenforceable, the distinction between commercial and military technology becomes less about security logic and more about strategic positioning.

The risk is concrete. Russia acquires, through routine commercial transactions, sensor fusion software that narrows its targeting gap in contested airspace. A non-state actor obtains dual-use components that when assembled, constitute a precision strike capability. Capabilities built over decades become accessible not through espionage but through ordinary trade, the kind that leaves no footprint and triggers no alarm until the military balance has already moved.

A functioning classification system would not eliminate these risks, but it would slow them. It would force adversaries to pay costs, in time, money, and exposure, that they currently do not have to pay. It would shift the burden of proof onto companies to demonstrate that their technology does not warrant control, rather than onto governments to prove that it does. It would mean the line is drawn by institutions with

security mandates, not by the parties with the most to gain from drawing it loosely.

Ultimately, a serious response would require treating classification as a strategic function rather than a compliance exercise. That means narrowing the definition of dual-use around capability and end-use rather than commercial origin, shifting more burden onto firms to justify permissive classifications, and giving security agencies greater authority to challenge or override company determinations before technologies reach foreign buyers. It would also require faster list updates and a clearer presumption that adaptable technologies such as artificial intelligence, autonomous systems, advanced sensors, and communications infrastructure should be reviewed for military effect before they are treated as ordinary commercial goods.

The question is not whether the current framework can be preserved. It cannot. The question is who redraws it, under what constraints, and accountable to whom. At the moment: largely private actors, very few constraints, and almost no one. That is not a sustainable basis for governing technologies that will shape the outcome of the next major conflict, and policymakers who have not grasped that urgency are not simply behind. They are running out of time.

Sumajja Denysiuk is a Junior Fellow at the Tech Policy Institute.

Who Draws the Line on Dual-Use Defense Technology? is a component of a series of op-eds penned by TPI Junior Fellows.

The appearance of U.S. Department of Defense (DoW) visual information does not imply or constitute DoW endorsement.

Sources

BIS imposes $5.8 million penalty against Pennsylvania company for shipments of low-level items to parties tied to the PRC's hypersonics, UAV, and military electronics programs. (2024, August 15). Bis.gov; Bureau of Industry and Security. https://www.bis.gov/node/20464

Chapman, J. (Ed.). (2022, September 8). Reliance on Dual-Use Technology Is a Trap. War on the Rocks. https://warontherocks.com/reliance-on-dual-use-technology-is-a-trap/

Definitions of Dual-use Related Concepts by the U.S. Department of Defense | AFCEA International. (2024, February 1). https://www.afcea.org/signal-media/technology/definitions-dual-use-related-concepts-us-department-defense

Freedberg, S. J. (2026, May). Pentagon clears 8 tech firms to deploy their AI on its classified networks. Breaking Defense. https://breakingdefense.com/2026/05/pentagon-clears-7-tech-firms-to-deploy-their-ai-on-its-classified-networks/

Gallo, M. (2021, June 28). The Global Research and Development Landscape and Implications for the Department of Defense. Congress.gov. https://www.congress.gov/crs-product/R45403

Heim, L. (2025, January 14). Understanding the Artificial Intelligence Diffusion Framework: Can Export Controls Create a U.S.-Led Global Artificial Intelligence Ecosystem? Rand.org; RAND Corporation. https://www.rand.org/pubs/perspectives/PEA3776-1.html

International Traffic in Arms Regulations: U.S. Munitions List Targeted Revisions. (2025, August 27). Federal Register. https://www.federalregister.gov/documents/2025/08/27/2025-16382/international-traffic-in-arms-regulations-us-munitions-list-targeted-revisions

Kania, E., & Laskai, L. (2021, January 28). Myths and Realities of China's Military-Civil Fusion Strategy. https://www.cnas.org/publications/reports/myths-and-realities-of-chinas-military-civil-fusion-strategy

What is the Wassenaar Arrangement? - The Wassenaar Arrangement. (2015). The Wassenaar Arrangement. https://www.wassenaar.org/the-wassenaar-arrangement/