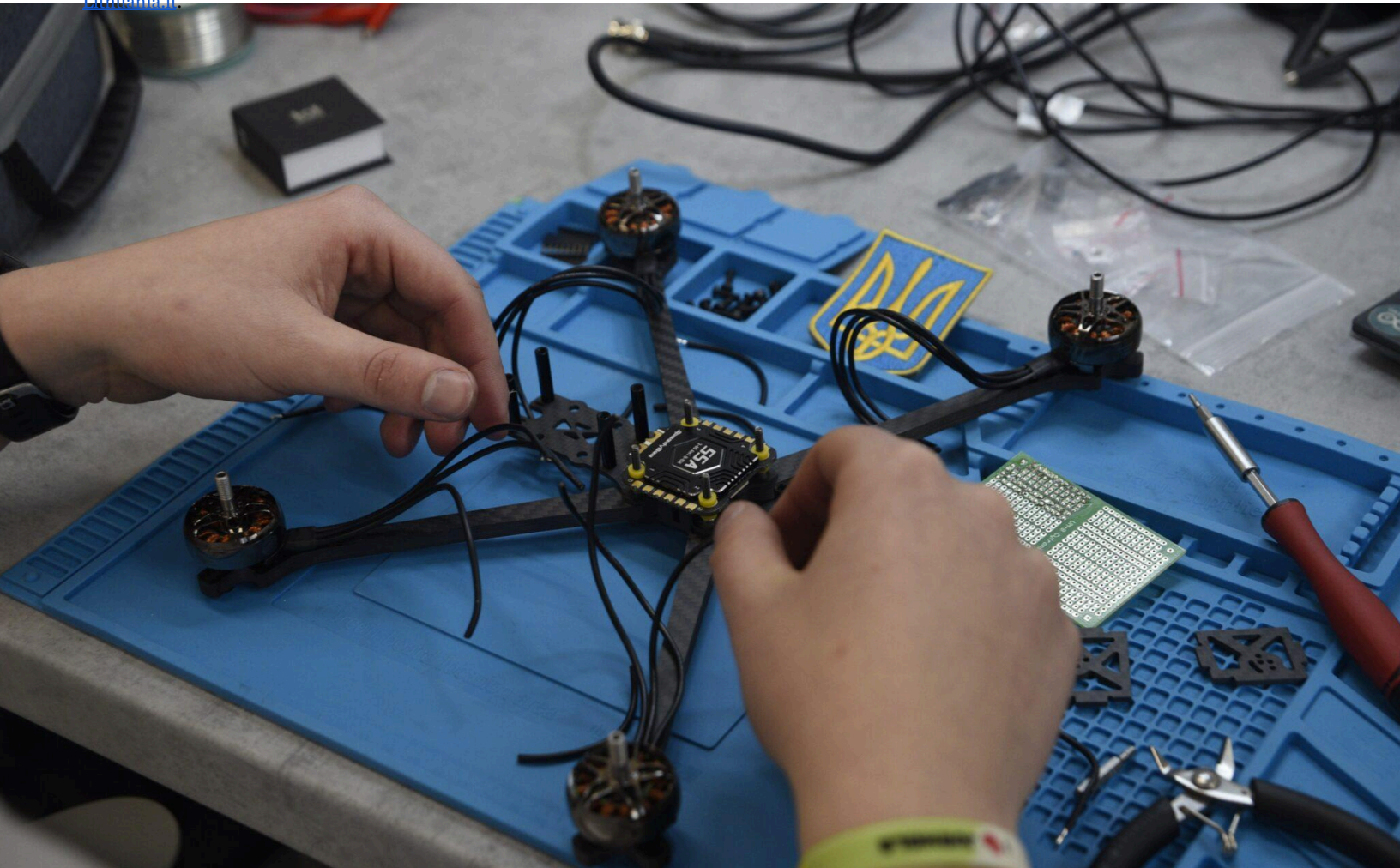




January 16th, 2026

Below the Threshold: Gaps in the UK Dual-Use Export Controls for Drone Components

Image source: Lithuania.lt, [“KTU M-Lab Students Build FPV Kamikaze Drones for Ukraine’s Defense”](#) (used for non-commercial purposes). © Lithuania.lt.



Members of the BRG Research Team

Theo Balavoine - Research Head, Sophomore, Princeton, NJ

Bridget Lonergan - Analyst, Junior, New York City, NY

Daniel Figueroa - Analyst, Sophomore, Miami, FL

Kanika Pachisia - Analyst, Sophomore, Mumbai, India

Simon Honig - Analyst, Senior, Seattle, WA

Oscar Knox - Analyst, Sophomore, Bethesda, MD

Tia Bhatnagar - Analyst, Sophomore, Mumbai, India

Aiden Wasserman - Editor, Sophomore, Westchester, NY

Sofia Shah - Editor, Sophomore, St. Louis, MO

About BRG

Boston Risk Group (BRG) is a student-led **pro bono** initiative based at Tufts University, offering research assistance to embassies, NGOs, and think tanks examining international issues. Our team of **26** highly motivated undergraduate researchers, studying fields such as international relations, economics, and data science, aims to foster meaningful collaborations with clients by delivering rigorous, policy-relevant, and implementable research. BRG is nonprofit, nonpartisan, and committed to assisting professional organizations. To learn more about BRG, visit bostonriskgroup.netlify.app

Research Integrity

Our mission to assist organizations through research and analysis is only possible through our unwavering commitment to the highest level of research accuracy and quality. To ensure our research and analysis are rigorous, objective, and accurate, we subject our research publications to a robust and exacting quality-assurance process through several rounds of sourcing verification.

BRG's publications do not necessarily reflect the opinions of its research clients, board of advisors, or members.

Published by Boston Risk Group, Medford, Massachusetts.

| Contents

| Abstract..... 4

| Context: The UK’s Drone Industrial Base.....5

| Regulatory and Framework Gaps..... 7

| Enforcement and Exploitation.....10

| Case Studies..... 14

| US and EU Dual-Use Export Frameworks.....18

| Recommendations..... 23

| References..... 25

| Abstract

The United Kingdom is focused on expanding its drone-industrial base as an economic and defense priority, yet its export-control regime still treats many drone-capable subsystems as ordinary commercial goods. Change is needed, as advocacy organizations have released explicit evidence of UK-made drone components implicated in explosive violence against citizens that were exported as uncontrolled goods. The rise of drone warfare has compounded these existing enforcement difficulties, making many off-the-shelf electronic components strategically significant.

This paper argues that the issue is primarily structural rather than enforcement-driven. The UK's export control legal framework permits the export of components that are functionally capable of integration into military drones with little or no scrutiny. Two specific legal gaps produce this outcome. First, the Strategic Export Control List relies on performance thresholds that exclude many commercially available components, even when those items are fully usable in military drones. Second, catch-all controls depend heavily on exporter self-classification, creating an environment where firms face strong incentives to self-declare "No License Required" to prioritize speed, cost savings, and plausible deniability over faithful adherence to catch-all controls. These incentives operate in practice through three recurring pathways: manipulating HS codes, intermediary routing that enables diversion and re-export, and documentation practices that emphasize benign end uses. The paper then grounds these mechanisms in three case studies of UK-origin components used in drones deployed in conflict zones, with each examining the relevant loophole that enabled its occurrence. Comparative case studies of the US and EU export control regimes follow this approach to identify the structural features that contribute to robust oversight and enforcement mechanisms. Finally, recommendations are provided for policy changes to increase UK oversight of below-military-grade drone components.

This paper makes a contribution that does not currently exist in the literature or policy debate by connecting several dimensions—including the legal framework, capacity of enforcement agencies, firm behavior, and existing evasion mechanisms—to provide a holistic explanation of why the UK export control regime fails to exercise meaningful oversight over uncontrolled drone components. Our findings provide UK policymakers and advocacy organizations with concrete recommendations for regulatory change.

| Context: The UK's Drone Industrial Base

As part of its Defense Industrial Strategy, the United Kingdom government is promoting drones and related technologies through state investment and workforce development programs as part of a broader effort to turn the defense sector into a driver of economic growth.¹ The UK drone sector is forecasted to contribute \$53 billion and generate over 600,000 new jobs by 2030. Furthermore, the UK's strength in high-value aerospace manufacturing, especially in engines, wings, and advanced aircraft systems, alongside having Europe's largest aerospace SME base, gives it a clear competitive edge in the global drone market.²

Drone-compatible imaging devices, such as thermal, low-light, and optical sensors, are often branded and used for civilian purposes such as inspection or mapping. Yet these exact sensor types are also indispensable to manufacturing drones suited to ISR (intelligence, surveillance, and reconnaissance) operations and kamikaze drones.³ Flight-control microcomputers—the onboard systems that process sensor data and translate commands into motor actions⁴—produced by UK firms have broad recreational and civilian applications, including FPV racing, recreational flying, aerial photography, and surveying, but have also been found in drones used in the Russo-Ukrainian War.⁵ This demonstrates how drone subsystems long associated with civilian and recreational use can be readily repurposed for military applications, making them inherently dual-use technologies.

Between 2021 and 2024, the United Kingdom provided significant drone technology, components, and surveillance equipment to major arms buyers such as Turkey, Israel, and Saudi Arabia. According to UK arms export data between 2021 and 2024, the UK authorized between £1 million and £4.5 million per year in arms and related licenses to 84 countries, 23 of which used explosive weapons in populated areas, causing tens of thousands of civilian deaths and injuries. UK-origin technology and

¹ “Export Controls: Dual-Use Items, Software and Technology, Goods for Torture and Radioactive Sources,” GOV.UK, accessed May 28, 2026, <https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources>.

² International Trade Administration, “United Kingdom - Aerospace and Defense,” International Trade Administration | Trade.gov, October 5, 2020, <https://www.trade.gov/country-commercial-guides/united-kingdom-aerospace-and-defense>.

³ “Infrared Imaging Solutions for UAVs, UGVs and Unmanned Systems,” Lynred, accessed May 28, 2026, <https://www.lynnred.com/UxS-market>.

⁴ “What Is a Drone Flight Controller?,” Grepow, accessed May 28, 2026, <https://www.grepow.com/blog/what-is-a-drone-flight-controller.html>.

⁵ Danai Nesta Kupemba, “British Parts Found in Russian Drones, Zelesnky Says,” BBC News, October 6, 2025, <https://www.bbc.com/news/articles/cg5e9zlpz6eo>.

components have supported foreign drone programs such as Turkey's Bayraktar series and Israeli drones implicated in the bombing of civilians.⁶

The UK's export-control regime is governed by the Export Control Order 2008, which establishes the framework for the types of goods to be classified as dual-use, while the Strategic Export Control List includes the specific goods subject to dual-use licensing requirements.⁷ Although under this framework, all drone components should be subject to dual-use licensing, the present regulatory system allows a significant quantity to be exported as uncontrolled goods, circumventing license requirements, making them commercially available. Reporting and investigations have documented commercial drone parts appearing in conflict drones in Gaza, Nagorno-Karabakh, and Ukraine.^{8,9,10} Thus, these components should be subject to a dual-use licensing regime because they can be repurposed for drones capable of operating in conflict zones.

Firms prefer to export their goods under civilian classifications for a variety of reasons. If a component is formally classified as dual-use, exporters must apply for licenses, complete end-use verification checks, and maintain extensive audit-ready documentation.¹¹ In practice, the export-licensing process can introduce delays and regulatory uncertainty, which may constrain firms' ability to pursue certain commercial opportunities or markets.¹²

⁶ Iain Overton, "Exporting Risk: How UK Arms Sales Overlap with Countries Using Explosive Weapons in Populated Areas," AOAV, July 20, 2025, <https://aoav.org.uk/2025/exporting-risk-how-uk-arms-sales-overlap-with-countries-using-explosive-weapons-in-populated-areas/>.

⁷ "The Export Control Order 2008," Legislation.gov.uk, accessed May 28, 2026, <https://www.legislation.gov.uk/ukxi/2008/3231/schedule/2/made/data.html>.

⁸ US targets Chinese companies over drone components used by Hamas, Houthis | Reuters, accessed May 28, 2026, <https://www.reuters.com/world/asia-pacific/us-targets-chinese-companies-over-drone-components-used-by-hamas-houthis-2025-10-08/>.

⁹ Matthew Ghazarian; Drone Empires: Ethnic Conflict, Techno-Spectacle, and Imperial Machinations Across Eurasia and Africa. *Comparative Studies of South Asia, Africa and the Middle East* 1 December 2025; 45 (3): 441–448. doi: <https://doi.org/10.1215/1089201X-12113388>

¹⁰ Ukraine races to make more war drone components at home | reuters, accessed May 28, 2026, <https://jp.reuters.com/article/world/ukraine-races-to-make-more-war-drone-components-at-home-idUSKBN319oHC/>.

¹¹ "Export Controls: Dual-Use Items, Software and Technology, Goods for Torture and Radioactive Sources," GOV.UK, accessed May 28, 2026, <https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources>.

¹² Kate Koren and Philip Luck, "Delays and Uncertainty in the Export Licensing Process: Findings from a CSIS Survey of U.S. Technology Exporters," CSIS, accessed May 28, 2026, <https://www.csis.org/analysis/delays-and-uncertainty-export-licensing-process-findings-csis-survey-us-technology>.

| Regulatory and Framework Gaps

This section analyzes the UK export control regime's legal framework to reveal two regulatory gaps that allow drone components with inherent dual-use functions to evade licensing requirements.

Performance-Based Thresholds

A major initial structural gap stems from the Strategic Export Control List's emphasis on performance-based thresholds, which allow goods with the functional capability to integrate into military drones to be exported without controls, provided they remain below certain performance thresholds. The Strategic Export Control List incorporates the Wassenaar Arrangement, a multilateral export control regime in which member states coordinate their national export control efforts to curb the spread of certain armaments.¹³ Wassenaar Categories 6 (Sensors and Lasers), 7 (Navigation and Avionics), and 9 (Aerospace and Propulsion) are particularly relevant because they encompass components commonly found in unmanned aerial vehicle (UAV) platforms. These categories control components only when they exceed specific performance levels. This use of performance-based thresholds reflects a regulatory approach intended to separate strategically sensitive goods from standard commercial products by imposing controls only when items meet defined performance criteria. It was further intended to avoid over-regulating mass-market commercial electronics in a technological context where strategically sensitive hardware was clearly distinguishable from consumer electronics.¹⁴

However, the challenge with export controls is that many commercially available drone components may have military relevance even when they do not meet the technical thresholds that trigger strict control under existing licensing rules. The UK Parliament does not address hobbyist drone components directly, but highlights a concern about the weaponization of smaller UAVs and the difficulty of scrutinizing future UAV development.¹⁵ In this context, a threshold-based system may leave some commercially available components outside stricter controls, even when they could later be integrated into military-capable drones. This should be understood primarily as a structural limitation of the export-control framework. Although there is no evidence that UK firms intentionally

¹³ List of dual-use goods and technologies and munitions list, accessed May 28, 2026, <https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf>.

¹⁴ *ibid*

¹⁵ "HC 1090 Towards the next Defence and Security Review," parliament.uk, accessed May 28, 2026, <https://publications.parliament.uk/pa/cm201314/cmselect/cmdfence/writev/1090/mo4.htm>.

design products to evade export controls, the reliance on technical thresholds can create regulatory gaps when civilian technologies can become usable in military systems.

Catch-All Controls

A second structural gap arises from the UK's catch-all controls, which rely on firms to self-assess whether their products require a license, with little scrutiny to ensure accurate compliance. While the UK has agencies such as HM Revenue & Customs (HMRC) to ensure that all goods on the Strategic Export Control List obtain the proper licenses, compliance for goods not on the list relies more heavily on exporters' own checks.¹⁶ To prevent the use of goods for military purposes, the UK uses a system of catch-all controls. Catch-all controls require firms to obtain a license to export their goods—even if they are not included on the Strategic Export Control List—if there is reason to believe that they will be used for a military purpose.¹⁷ However, the onus of determining whether those goods might be used for a military purpose rests with the firm itself, and if a firm self-assesses that an export is “No License Required” (NLR), there is limited official scrutiny of the export's destination and purpose.¹⁸ In practice, this creates a permissive environment in which exporters' interpretations of the end-user play a decisive role in determining whether a component enters global supply chains without scrutiny.

It is true that exporters can lack visibility into downstream uses of commercial electronic goods, and many intermediary destinations do not raise immediate red flags. However, exporting firms can also take measures to conceal the extent of their knowledge of downstream buyers and their purposes, and consciously forgo applying for a license even when they are legally required to do so. Given that this system of catch-all controls creates a payoff structure in which the benefits of an expedited process and cost savings far outweigh the low likelihood of being caught, it is rational for firms to evade the UK catch-all controls. As a result of the emphasis on firms self-classifying, the catch-all mechanism captures only a narrow subset of UAV-capable components that fall below control thresholds, yet nonetheless contribute to military drone manufacturing.

¹⁶ “Export Controls: Dual-Use Items, Software and Technology, Goods for Torture and Radioactive Sources,” GOV.UK, accessed May 28, 2026, <https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources>.

¹⁷ *ibid*

¹⁸ *ibid*

Recap

When these two structural issues are combined, the present result is that the majority of drone components fall below the Strategic Export Control List's technical thresholds and can therefore be exported as uncontrolled goods, receiving little oversight beyond a weak legal obligation to self-report potential violations of catch-all controls.

Taken together, these gaps highlight deeper structural issues within the UK export control regime. The lists of dual-use goods were originally developed at a time when military hardware was clearly distinguishable, and the emphasis on technical thresholds was intended to ensure predictability while reducing regulatory burdens on commercial industry.²² However, modern UAV systems heavily utilize commercially available components that were not considered strategically significant when these frameworks were established.²³ This dynamic is reinforced by the limited effectiveness of catch-all controls due to the pitfalls of exporter self-classification. These are not enforcement-related issues; rather, they are deep, structural deficiencies. This structural misalignment lays the groundwork for understanding the common loopholes UK firms abuse to export inherently dual-use drone components as uncontrolled goods.

| Enforcement and Exploitation

Most drone component manufacturing firms export products below the technical thresholds of the Strategic Export Control List and, therefore, are only subject to catch-all controls, under which they must apply for a license if there is reason to believe their goods will be used for military purposes. This section begins by arguing that weak enforcement frameworks heavily influence firms' behavior by incentivizing them to prioritize evading oversight and feigning innocence if caught, rather than effectively deterring violations of catch-all controls in the first place. This section then analyzes three ways firms abuse this loophole to export uncontrolled goods for military purposes while hiding their tracks and creating a purported sense of innocence.

The Civilian Blindspot

The UK export control regime's limited and fragmented enforcement capacity may create opportunities for firms to evade catch-all controls or avoid close scrutiny, particularly where exporters classify goods as not requiring a license. Under catch-all controls, exporters are legally required to seek a license if they have reason to suspect their products might be used for military purposes. The Export Control Joint Unit (ECJU) reviews the details of shipments of uncontrolled goods only when exporters voluntarily seek a license or request guidance.¹⁹ Therefore, a silent majority of products exported by firms that self-declare as NLR evade the scrutiny of the ECJU entirely.

Once an exporter designates a shipment as NLR, responsibility shifts to HMRC, which is tasked with investigating and enforcing export-control law to ensure accurate compliance with catch-all controls.²⁰ Critically, when firms are caught violating catch-all controls, criminal prosecution requires proof of conscious intent to subvert catch-all controls. Because this evidentiary threshold is difficult to satisfy, it is often difficult to prosecute firms even when violations are identified. This policy may have incentivized exporters to characterize violations of catch-all controls as accidental errors, thereby mitigating legal repercussions.²¹ In 2023, for instance, HMRC and Border Force reported 266 seizures

¹⁹ "How the United Kingdom Approaches Export Controls," Global Investigations Review, accessed May 28, 2026, <https://globalinvestigationsreview.com/guide/the-guide-sanctions/sixth-edition/article/how-the-united-kingdom-approaches-export-controls>.

²⁰ Tom Stocker, "UK Signals Increased Export Control Enforcement and Penalties," Pinsent Masons, December 5, 2025, <https://www.pinsentmasons.com/out-law/analysis/uk-increased-export-control-enforcement-penalties>.

²¹ "UK Sanctions Guidance for Non-UK Businesses," GOV.UK, accessed May 28, 2026, <https://www.gov.uk/guidance/uk-sanctions-guidance-for-non-uk-businesses>.

of misclassified goods and 260 voluntary disclosures, yet secured only 15 criminal prosecutions.²² This gap suggests that British firms could be exploiting weaknesses in the catch-all system to avoid scrutiny and preserve plausible deniability if their exports are later called into question.²³

Harmonized System

To evade detection for violating catch-all controls, exporters could take advantage of the Harmonized System (HS), a globally standardized system for classifying goods, to shape HMRC's perception of their goods. However, by categorizing goods according to broad physical characteristics, HS codes compound the opaqueness of exports. For example, exporters may select classifications that make uncontrolled drone components with potential military applications appear benign, reducing the likelihood of scrutiny.²⁴

HS code 8542.31 illustrates this problem. This umbrella category encompasses both low-value consumer microcontrollers and high-performance processors recovered from Russian guidance systems.²⁵ The UK–US Common High Priority Items List (CHPL) lists 8542.31 as a Tier 1 item of “the highest concern,” yet because it is commonly found in civilian electronics, it continues to be treated as a standard commercial code at the border.²⁶ The UK has still not embedded this Tier-1 risk into routine customs screening, instead relying on general due diligence, leaving most 8542.31-coded items to move under the presumption of civilian trade.²⁷

End-Use Verification & Re-Exporting

²²“How the United Kingdom Approaches Export Controls,” Global Investigations Review, accessed May 28, 2026, <https://globalinvestigationsreview.com/guide/the-guide-sanctions/sixth-edition/article/how-the-united-kingdom-approaches-export-controls>.

²³ Critically, the weak enforcement capacity of the HMRC illustrates how little deterrence the current enforcement model provides for firms to stop violating catch-all controls. While the Office of Trade Sanctions Implementation (OTSI) was created in 2024 to strengthen civil enforcement, its remit is narrowly focused on sanctions rather than systematic auditing of high-volume electronics exports, such as the integrated circuits appearing in Russian weapons systems.

²⁴“UK Export Controls,” Global Sanctions, December 16, 2025, <https://globalsanctions.com/sanctioning-states/uk/export-controls-3/>.

²⁵“HS-Code List,” The Dollar Business, accessed May 28, 2026, <https://in.thedollarbusiness.com/hs-codes/electronic-integrated-circuits-processors-controllers/section-16/chapter-854231>.

²⁶“Bureau of Industry and Security,” Licensing, accessed May 28, 2026, <https://www.bis.gov/licensing/country-guidance/common-high-priority-items-list-chpl>.

²⁷“Export Controls: Military Goods, Software and Technology,” GOV.UK, accessed May 28, 2026, <https://www.gov.uk/guidance/export-controls-military-goods-software-and-technology>.

A central weakness enabling firms to circumvent catch-all controls is the lack of end-use verification measures. When exporters apply for a military or dual-use Standard Individual Export License (SIEL), they must submit an End-User and Stockist Undertaking (EUSU) form to identify the final user.²⁸ However, uncontrolled shipments do not require an EUSU. The absence of this documentation eliminates the evidence necessary to prove that firms consciously knew the final destination and use of their exports in a prosecution. The lack of end-use verification has enabled firms to evade being caught and preserve their purported innocence in two ways.

Firstly, firms often use intermediaries in other countries to claim plausible deniability regarding their association with the end-user. Exporters often ship items to non-embargoed jurisdictions, such as Kazakhstan, Turkey, or the UAE, which serve as transshipment hubs that facilitate diversion into sanctioned nations.²⁹ Intermediaries create front companies that appear legitimate, and despite UK government guidance on "red-flag" indicators (such as residential business addresses), these entities routinely purchase sensitive microelectronics. Because the UK conducts no routine post-shipment verification (PSV) checks on uncontrolled goods, there is no mechanism to verify, for example, whether items declared for "industrial monitoring" were not diverted to military drone manufacturers. Similarly, because exporters aren't required to complete an EUSU, if HMRC attempts to prosecute a firm, exporters can maintain their innocence by stating that they were unaware of the end user's identity.

Although UK firms might not necessarily want their products to end up in embargoed destinations, they are aware of where their products go, and dealing with intermediaries allows them to maintain plausible deniability while still making a profit. Regardless, the UK has not yet incorporated these shortcomings into updated procedures: shipments through known transshipment hubs do not automatically trigger an ECJU review or enhance HMRC due diligence.

Secondly, regarding invoices, audits, and other export-tracking documents, firms may place emphasis on the export's final commercial uses. Intermediary firms may describe imports in export documents using benign purposes, such as agricultural surveying or industrial monitoring. While such

²⁸"End-User and Stockist Undertaking (EUSU) Form Guidance," GOV.UK, accessed May 28, 2026, <https://www.gov.uk/government/publications/end-user-undertaking-euu-form/end-user-undertaking-euu-form-guidance>.

²⁹"Countering Russian Sanctions Evasion - Guidance for Businesses," GOV.UK, accessed May 28, 2026, <https://www.gov.uk/government/publications/countering-russian-sanctions-evasion-and-circumvention/countering-russian-sanctions-evasion-guidance-for-exporters>.

descriptions may satisfy formal documentation, they can also make it more difficult for HMRC to demonstrate the requisite knowledge threshold for prosecution.

Recap

In conclusion, a combination of the ECJU placing the onus of self-classification on firms and a lack of required documentation results in a weak oversight framework that can incentivize firms to evade the requirements of catch-all controls. Firms can employ several methods, including adopting ambiguous HS codes, using intermediary nations, and emphasizing the supposed commercial purposes of their exports. If firms' components are documented in conflict zones, the lack of end-user verification measures and firms' extensive efforts to conceal their awareness of violations make it nearly impossible to convict firms of knowingly violating catch-all controls.

| Case Studies

The continued diffusion of UK-made drone components into contemporary conflict zones has raised persistent questions about the adequacy of the UK's export control regime. Although UK law maintains extensive restrictions on military and dual-use technologies, manufacturers continue to ship ostensibly civilian parts abroad under uncontrolled classifications. These items, once exported, have repeatedly been incorporated into weapons systems deployed in active hostilities. The following section presents three illustrative case studies of uncontrolled UK-made drone components that appear in conflict zones and analyzes the legal and enforcement deficiencies that enable each instance.

Case Study One: Lack of End-User Certification

In 2020, an Armenian National Committee of America report identified Andair Ltd FS20 Type-1 fuel valves inside Turkish Bayraktar TB2 drones used by Azerbaijan during the ongoing Nagorno-Karabakh conflict.³⁰ UK authorities stated that no export licenses had been granted to Azerbaijan, which had been previously subject to an arms embargo.³¹ Given that Azerbaijan was under an arms embargo, the most likely explanation of how UK-made drone components ended up being used by the Azerbaijani military is that the components were integrated into drones and then re-exported.

Andair's fuel valve is below the thresholds outlined in the Strategic Export Control List, but because Baykar is a defense company, it is highly unlikely that Andair evaded catch-all controls and presumably obtained a SIEL. However, once incorporated into TB2s, these products were re-exported to Azerbaijan without the knowledge of UK authorities. Andair stopped supplying Baykar after the Embassy of Armenia, on 02/11/2020, contracted the company to stop supplying parts for armed drones and terminated its relationship with Baykar to comply with UK export controls.³²

³⁰Evidence of U.S. parts in Turkish drones deployed by Azerbaijan, accessed May 28, 2026, https://anca.org/assets/pdf/BayraktarDrone_US_Nato_Technology.pdf.

³¹"[Withdrawn] UK Arms Embargo on Armenia and Azerbaijan," GOV.UK, July 2, 2025, <https://www.gov.uk/guidance/uk-arms-embargo-on-armenia-and-azerbaijan>.

³²Murat Sofuoglu, "TRT World - Will Turkey's Drone Industry Be Affected by UK Firm's Cut in Exports?," TRT World, May 3, 2023, <https://www.trtworld.com/magazine/will-turkey-s-drone-industry-be-affected-by-uk-firm-s-cut-in-exports-43292>.

Case Study Two: Interpretive Decontrol

In 2025, investigative reporting revealed that Israeli Aerospace Industries' APUS-25 quadcopter, which has been used in strikes in Gaza, was equipped with heavy-fuel engines produced by Dorset-based RCV Engines.³³ The pathway enabling this outcome can largely be traced to regulatory decontrol. In 2022, the UK government removed RCV's gasoline and heavy-fuel four-stroke UAV engines from the military export list. According to RCV, their engines were "now free from export license controls," enabling them to be shipped globally without a SIEL.³⁴ However, public records and official replies complicate the narrative: a written parliamentary question to the Department for Business and Trade clarified that the only formal amendments to the propulsion-engine control entry (ML10.d / 9A001) since 2020 concerned aero-engines manufactured before 1946, and did not decontrol engines designed for UAVs.³⁵ Therefore, while RCV claimed their engines were unrestricted, the government may not have formally removed them from the list. One plausible explanation for this contradiction is that the engines were deemed to fall below the "specially designed for military use" threshold, allowing RCV to export them through commercial channels or under Open General Export Licenses without SIELs or end-user certification.³⁶

In practice, this decontrol created a seamless pathway into commercial export channels, enabling continued downstream military integration due to a lack of end-user certification for uncontrolled goods. The lack of licensing obligation allowed Israeli Aerospace Industries to integrate RCV engines into the APUS-25 platform without regulatory oversight.³⁷ Even after the UK suspended around thirty export licenses to Israel in late 2024, RCV's products continued to move freely, unaffected by the broader restrictions.³⁸ BBC reporting indicates that the engines were sold under a claimed export exemption, creating a gap in oversight that allowed them to move through commercial channels without the scrutiny normally associated with arms exports.³⁹ The RCV case exemplifies how deliberate removal or interpretive decontrol from export control lists creates sweeping licence exemptions with significant security implications. This case also highlights the inherent issues with

³³ John McEvoy, "Israel's Killer Drones Powered with UK Engines," Declassified UK, April 28, 2025, <https://www.declassifieduk.org/israels-killer-drones-powered-with-uk-engines/>.

³⁴ *ibid*

³⁵ "Unmanned Air Systems: Question for Department for Business and Trade," UK Parliament, May 14, 2025, <https://questions-statements.parliament.uk/written-questions/detail/2025-05-14/52328>.

³⁶ *ibid*

³⁷ "Revealed: How British Engines Ended up in Israeli Drones," Declassified UK, December 11, 2025, <https://www.declassifieduk.org/revealed-how-british-engines-ended-up-in-israeli-drones/>.

³⁸ *ibid*

³⁹ Jamie Morris, "Dorset MP Seeks Clarity over Arms Exports to Israel," BBC News, June 5, 2025, <https://www.bbc.com/news/articles/cg5v1ljy6ngo>.

not requiring end-user certification for all uncontrolled drone components being exported to a high-risk country such as Israel.

Case Study Three: Failure of Catch-all Controls

Recently, the president of Ukraine, Volodymyr Zelenskyy, publicly stated that on the nights of October 4th and 5th, 2025, Russia used 549 weapons containing 100,688 foreign-made components, including UAVs with UK-made avionics and microcontrollers.⁴⁰ The UK has formally banned all direct exports of military items to Russia since 2014 and stated that “it is making every effort to stop British companies from exporting components for weapons production to Russia,” and that it takes these reports “extremely seriously.” but would look into the issue nonetheless.⁴¹

Investigations into Russian Orion, Shahed-variant, and Lancet UAVs repeatedly show that once sold to third-country clients, such as Kazakhstan, such components are re-exported into Russia’s drone program without triggering UK oversight.⁴² For example, Kazakhstan’s exports of microchips and semiconductors to Russia jumped from \$245,000 in 2021 to \$18 million in 2022, demonstrating the exponential increase in re-exports to Russia.⁴³

This case highlights several issues with the UK export control regime. These avionics and microcontrollers are functionally capable of integration into military use drones but fall below the performance-based thresholds that would classify them as dual-use components under the Strategic Export Control List. Because firms can export these components on uncontrolled schedules, they are subject to little scrutiny and only to catch-all controls, requiring a license only if there is reason to suspect the product will be used for military purposes. By utilizing intermediary countries and exporting under traditionally commercial HS codes, firms can maintain plausible deniability of requisite intent to violate catch-all controls if their products are found in Russian UAVs. Had all firms exporting items functionally capable of UAV-integration to high-risk re-exporting destinations been

⁴⁰Ukraine’s Zelenskyy says western parts found in Russian drones, missiles | Russia-Ukraine War News | Al Jazeera, accessed May 28, 2026, <https://www.aljazeera.com/news/2025/10/6/ukraine-zelenskyy-says-western-parts-found-in-russian-drones-missiles>.

⁴¹ *ibid*

⁴²Benjamin Bidder (Der Spiegel) Reported by Maria Zholobova (IStories), “Kazakhstan Has Become a Pathway for the Supply of Russia’s War Machine. Here’s How It Works.,” OCCRP, May 7, 2026, <https://www.occrp.org/en/investigation/kazakhstan-has-become-a-pathway-for-the-supply-of-russias-war-machine-here-s-how-it-works>.

⁴³Frontline report: Ukraine Strikes Deep into Russia’s “untouchable” Caspian Sea, disabling oil platforms and military barges - euromaidan press, accessed May 28, 2026, <https://euromaidanpress.com/2025/12/23/frontline-report-2025-12-23/>.

required to submit end-user certification forms, the transfusion of UK-made drone components into Russia would become far more difficult. This case provides a concrete example of an increase in re-exports of drone components to Russia as firms could evade catch-all controls through intermediary firms and ambiguous HS codes.

| US and EU Dual-Use Export Frameworks

This section examines the dual-use export control frameworks of the United States and the European Union, focusing especially on how each system governs inherently dual-use drone components. The purpose is to identify the regulatory strengths within the US and EU models and assess the extent to which similar mechanisms exist, or do not exist, within the United Kingdom's export control regime. This analysis provides a comparative basis for understanding where the UK framework aligns with leading international practice and where structural differences emerge.

United States Dual-Use Framework

The US oversees dual-use exports under the Export Administration Regulations (EAR), administered by the Bureau of Industry and Security (BIS).⁴⁴

The US system is characterized by a combination of entity-based controls, broad catch-all rules, stringent end-user screening, extraterritorial jurisdiction, and strong enforcement infrastructure. Together, these features enable the US to regulate dual-use drone components more aggressively than many other countries.

Classification

The US governs the licensing requirements for dual-use items through the Commerce Control List (CCL) through an Export Control Classification Number (ECCN).⁴⁵ Many components that could be used in more advanced drones are governed under ECCN's with strict licensing requirements. For example, thermal imagery cameras contained in ECCN 6A003.b.4 are subject to Regional Stability controls that impose licensing requirements for exports and reexports to any country other than Australia, Canada, or the UK.⁴⁶

All items not found on the CCL are subject to the generic classification EAR99, which generally contains lower-technology, widely traded consumer goods that do not require a license in most

⁴⁴"Bureau of Industry and Security," EAR, accessed May 29, 2026, <https://www.bis.gov/regulations/ear>.

⁴⁵"(ECCN) and Export Administration Regulation (EAR99)," International Trade Administration | Trade.gov, accessed May 28, 2026, <https://www.trade.gov/eccn-and-export-administration-regulation-ear99>.

⁴⁶ Code of Federal Regulations, Title 15: Commerce and Foreign Trade, accessed May 28, 2026, <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C>.

scenarios but are subject to US catch-all controls.⁴⁷ Less-advanced drone components likely to be found in inexpensive FPV systems are likely to be subject to the generic classification EAR99.

Similarly, the UK governs dual-use goods through its Strategic Export Control List and goods falling below those technical thresholds are governed through UK catch-all controls. However, US catch-all controls are structurally far more effective than the UK's.

Catch-all Controls

BIS catch-all controls require US firms to seek a license if any seemingly harmless EAR99 item is being exported to an entity on any of the US's entity-based lists. The BIS maintains several lists to identify known high-risk and military entities, such as the Entity List, Denied Persons List, Unverified List, and Military End-User List.⁴⁸ This objective system, which focuses on who the buyer is, removes any question about whether the exporter had reasonable grounds to suspect military use. Similarly, the onus of identifying high-risk firms with potential military end-use rests with the BIS, which is responsible for consistently updating entity-based lists.

On the other hand, UK catch-all controls require firms to notify HMRC only if they suspect a military end-use or if the entity is present on the UK Sanctions List.⁴⁹ However, the UK only maintains the UK Sanctions List and does not maintain a list similar to the US entity list, which contains high-risk entities, greatly reducing the number of firms that would trigger immediate flagging by HMRC.⁵⁰ Therefore, in the absence of comprehensive lists of high-risk firms and entities, the onus of determining high-risk end-use falls on the exporting firm itself, thereby incentivizing evasion.

The US's emphasis on maintaining expansive end-user-based controls rather than relying on firms to identify potential military end-use is structurally more effective in ensuring ostensibly civilian products are not incorporated into military products or diverted.

De Minimis Extraterritorial Rule

⁴⁷“(ECCN) and Export Administration Regulation (EAR99),” International Trade Administration | Trade.gov, accessed May 28, 2026, <https://www.trade.gov/eccn-and-export-administration-regulation-ear99>.

⁴⁸“Guidance on End-User and End-Use Controls and U.S. Person Controls,” Bureau of Industry and Security, accessed May 28, 2026, <https://www.bis.gov/licensing/guidance-on-end-user-and-end-use-controls-and-us-person-controls>.

⁴⁹“Military End-Use Controls,” GOV.UK, accessed May 28, 2026, <https://www.gov.uk/guidance/military-end-use-controls>.

⁵⁰“UK Strategic Export Controls,” GOV.UK, accessed May 28, 2026, <https://www.gov.uk/guidance/uk-strategic-export-controls>.

The US applies a de minimis jurisdiction rule under the EAR—called FDPR rules—whereby foreign-manufactured items that incorporate a threshold level of US origin-controlled content remain subject to US export control authority, even when produced entirely outside the US.⁵¹ This rule enables US regulators to exert extraterritorial legal control over foreign drone manufacturing firms that incorporate US-origin components or technology. This rule is particularly critical when dealing with re-exports. A foreign company that imports a US-origin component still needs US authorization to re-export it or integrate it into military equipment meant for export.⁵²

The UK does not have an equivalent de minimis jurisdiction rule. UK-origin components incorporated abroad typically fall outside UK control unless the finished product is re-exported directly from the UK.⁵³ Thus, this powerful US regulatory tool has no UK parallel.

European Union Dual-Use Framework

The EU regulates dual-use exports through Regulation (EU) 2021/821, which combines list-based controls with expanded catch-all authorities and new provisions on cyber-surveillance and misuse related to human rights.⁵⁴ The EU framework is unique in integrating normative considerations, such as repression, privacy violations, and internal security abuses, into traditional export control logic.

Annex I Classification System

The EU regulates dual-use exports under Regulation (EU) 2021/821 (EU Dual-Use Regulation), which governs the export, transfer, brokering, transit, and technical assistance of dual-use goods, software, and technology.⁵⁵ The EU maintains a common dual-use items list (Annex I) that includes electronics, sensors, avionics components, and other sensitive technologies, which require prior authorization.⁵⁶ The UK still uses the retained Annex I from EU law. In terms of classification thresholds and list structure, the UK is almost identical to the EU system.

⁵¹“Code of Federal Regulations Title 15 Subchapter C 734.4,” Code of Federal Regulations, accessed May 29, 2026, <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.4>.

⁵²“UK Strategic Export Controls,” GOV.UK, accessed May 28, 2026, <https://www.gov.uk/guidance/uk-strategic-export-controls>.

⁵³“Extraterritorial Applications in Export Controls: EU, UK, US, and Cn – What to Consider,” Export controls EU, UK, US, CN: Extraterritoriality aspects, accessed May 28, 2026, <https://www.aeb.com/en/magazine/articles/extraterritoriality-export-controls-us-uk-eu-cn.php#uk>.

⁵⁴Regulation (EU) 2021/821 - EUR-lex, accessed May 29, 2026, <https://eur-lex.europa.eu/eli/reg/2021/821/oj>.

⁵⁵ *ibid*

⁵⁶“Winston Pocket Guide to EU Export Control and Regulation,” Winston & Strawn, accessed May 29, 2026, <https://www.winston.com/en/blogs-and-podcasts/european-regulatory-compass/winston-pocket-guide-to-eu-export-control-and-regulation>.

Article 4 Catch-All Controls

This feature allows EU Member States to impose controls on non-listed items if exporters know or suspect they may be used for military end-use in embargoed states, internal repression, terrorism, or destabilizing surveillance.⁵⁷ It broadens control over civilian-classified items while enabling responsiveness to emerging drone-adapted technologies.

The UK's catch-all is based on the same pre-Brexit EU framework, but post-Brexit, it has not expanded in scope as the EU did in a 2021 revamp of export control laws.⁵⁸

Article 5 (Cyber-Surveillance Catch-All)

The EU has a unique provision allowing restrictions on non-listed cyber-surveillance tools—including some drones—that could be used for human-rights violations.⁵⁹ This provision recognises that drone technology can be misused not only in military contexts but also in human-rights-sensitive policing and repression.

The UK has no equivalent standalone cyber-surveillance catch-all. The UK does prohibit exports that directly support internal repression, but it does not impose a general obligation covering non-listed cyber-surveillance items.⁶⁰

Exporter Due-Diligence Requirement

EU exporters must implement internal compliance programs (ICPs) and conduct due-diligence assessments when exporting potentially high-risk technologies, even when uncontrolled.⁶¹ This law shifts part of the responsibility for risk assessment to the private sector, improving early detection of problematic end users.⁶²

⁵⁷ “Dual-Use Items,” Bundesministerium für Wirtschaft, Energie und Tourismus, accessed May 29, 2026, <https://www.bmwet.gv.at/en/Topics/Export-Control/Export/Dual-Use.html>.

⁵⁸ “An Overview of the Recast EU Dual Use Regulation,” Covington & Burling LLP, accessed May 29, 2026, <https://www.cov.com/en/news-and-insights/insights/2021/09/an-overview-of-the-recast-eu-dual-use-regulation>.

⁵⁹ Regulation - 2021/821 - en - EUR-lex, accessed May 28, 2026, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021Ro821>.

⁶⁰ “UK Strategic Export Controls,” GOV.UK, accessed May 28, 2026, <https://www.gov.uk/guidance/uk-strategic-export-controls>.

⁶¹ “New EU Dual-Use Regulation Increases Focus on Internal Compliance Programmes,” Taylor Wessing, September 2, 2024, <https://www.taylorwessing.com/en/insights-and-events/insights/2021/09/neue-eu-dual-use-verordnung-erhoeht-den-fokus-auf-interne-compliance-programme>.

⁶² Raminta Dereskeviciute, “EU Member States Implement Additional Measures to Regulate Export of Non-Listed Dual-Use Items,” *The National Law Review*, October 4, 2024,

The UK encourages compliance programs but does not require them.⁶³ There is no mandatory due diligence obligation for exports of uncontrolled drone components. A lack of compliance programs in the UK is a major driver of UK firms' conscious decision to subvert catch-all controls.

<https://natlawreview.com/article/eu-member-states-implement-additional-measures-regulate-export-non-listed-dual-use>.

⁶³“Compliance Code of Practice for Export Licensing,” GOV.UK, accessed May 28, 2026, <https://www.gov.uk/government/publications/export-control-compliance-code-of-practice/compliance-code-of-practice-for-export-licensing#:~:text=This%20code%20is%20voluntary>.

| Recommendations

Based upon a comprehensive review of the UK's export control regime, common loopholes exploited by firms, case studies of uncontrolled components found in conflict-zone drones, and the US and EU legal and enforcement frameworks, several recommendations could be implemented to improve the UK's system.

The UK government should reform the legal framework of its export control regime in several ways:

- ❖ **First**, the UK Strategic Export Control List should be updated to incorporate **function-based thresholds** alongside performance-based ones, to ensure that all UAV-compatible components are subject to ECJU oversight. Many cases of low-performance components being exported on uncontrolled schedules, with little scrutiny, and later found incorporated into military FPV drones highlight the need for function-based controls. The UK could model this system on the US ECCN system, which establishes a separate category for components that are drone-compatible but not “military-grade” and are subject to greater oversight.
- ❖ **Second**, the UK should expand its list of **high-risk entities and intermediaries**, which remains far less expansive than the US and EU.
- ❖ **Third**, the UK should reform its **catch-all controls** to require that any goods exported to a listed entity be licensed. The current UK system, prioritizing reasonable suspicion of final military use, is highly subjective and incentivizes exploitation. On the other hand, a list-based system is entirely objective and enables far greater breadth, as any component destined for a high-risk entity, regardless of performance, is subject to oversight.
- ❖ **Fourth**, restrict or revoke the use of **Open General Export Licenses that require less end-user certification for drones, drone components, and related software, and instead require** case-by-case SIELs.

The UK government should reform oversight procedures and the relevant agencies in several ways:

- ❖ **First**, any drone component exported to **conflict-affected or high-risk intermediary states** should be subject to enhanced oversight and scrutiny, regardless of an exporter's NLR self-classification. This should be implemented through mandated **end-user certification** and **post-shipment verification**, including occasional random checks on uncontrolled goods. Doing so would ensure items reach the listed user, are used for the given purpose, and are not re-exported, as it occurred in the Turkish Bayraktar TB2 incident.

- ❖ **Second**, the UK should strengthen cooperation between the presently disjointed ECJU, which sets licensing requirements, and HMRC, which enforces and investigates export-control violations. This could be done by publishing a yearly joint strategy outlining enforcement focus areas and priority technologies to align efforts. Furthermore, the ECJU could also automatically notify HMRC when exporters self-declare NLR for high-risk goods or routes to increase scrutiny.
- ❖ **Third**, the UK should restore the now-defunct Committees on Arms Export Controls, which was tasked with scrutinizing government policy on arms licensing with a focus on conflict risks and preventing complicity in human-rights abuses.⁶⁴ In 2024, the Committees on Arms Export Control was disbanded and replaced with a far smaller sub-committee within the Business and Trade Committee.⁶⁵
- ❖ **Fourth**, the process by which firms petition to have their product removed from controlled item lists must be reformed to increase public oversight. Currently, if the government approves a firm's petition for removal from controlled items lists—typically due to lobbying—, there is no requirement to publicly disclose a rationale, which occurred in the RCV Engines case. Additionally, petition requests should be subject to review from independent technical experts to ensure that decontrol decisions are made based on objective facts rather than political lobbying.

The UK government must take targeted action to stop the flow of strategically sensitive microelectronics to Russia through transshipment hubs by implementing several reforms:

- ❖ **First**, all Common High Priority List Tier 1–2 goods exported to known transshipment hubs should be subject to **mandatory ECJU review**, even when firms self-classify NLR.
- ❖ **Second**, if the ECJU requires a Tier 1-2 good to obtain a SIEL, exporting firms should be required to submit not only an end-user undertaking but also conduct **post-shipment verification** to prevent diversion.
- ❖ **Third**, establish a dedicated Tier 1–2 **monitoring agency** to execute PSV checks.

⁶⁴ Committees on arms export controls - summary - committees - UK parliament, accessed May 29, 2026, <https://committees.parliament.uk/committee/15/committees-on-arms-export-controls>.

⁶⁵ Business and Trade Sub-Committee on Economic Security, Arms and Export Controls - Membership - Committees - UK parliament, accessed May 29, 2026, <https://committees.parliament.uk/committee/783/business-and-trade-subcommittee-on-economic-security-arms-and-export-controls/membership/>.

References

“An Overview of the Recast EU Dual Use Regulation.” Covington & Burling LLP. Accessed May 29, 2026.

<https://www.cov.com/en/news-and-insights/insights/2021/09/an-overview-of-the-recast-eu-dual-use-regulation>.

“Bureau of Industry and Security.” EAR. Accessed May 29, 2026.

<https://www.bis.gov/regulations/ear>.

“Bureau of Industry and Security.” Licensing. Accessed May 28, 2026.

<https://www.bis.gov/licensing/country-guidance/common-high-priority-items-list-chpl>.

Business and trade sub-committee on economic security, arms and export controls - membership - committees - UK parliament. Accessed May 29, 2026.

<https://committees.parliament.uk/committee/783/business-and-trade-subcommittee-on-economic-security-arms-and-export-controls/membership/>.

“Code of Federal Regulations Title 15 Subchapter C 734.4.” Code of Federal Regulations. Accessed May 29, 2026.

<https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.4>.

Code of Federal Regulations, Title 15: Commerce and Foreign Trade. Accessed May 28, 2026.

<https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C>.

Committees on arms export controls - summary - committees - UK parliament. Accessed May 29, 2026.

<https://committees.parliament.uk/committee/15/committees-on-arms-export-controls>.

“Compliance Code of Practice for Export Licensing.” GOV.UK. Accessed May 28, 2026.

<https://www.gov.uk/government/publications/export-control-compliance-code-of-practice/compliance-code-of-practice-for-export-licensing#:~:text=This%20code%20is%20voluntary>.

“Countering Russian Sanctions Evasion - Guidance for Businesses.” GOV.UK. Accessed May 28, 2026.

<https://www.gov.uk/government/publications/countering-russian-sanctions-evasion-and-circumvention/countering-russian-sanctions-evasion-guidance-for-exporters>.

Dereskeviciute, Raminta. “EU Member States Implement Additional Measures to Regulate Export of Non-Listed Dual-Use Items.” *The National Law Review*, October 4, 2024.

<https://natlawreview.com/article/eu-member-states-implement-additional-measures-regulate-export-non-listed-dual-use>.

“Dual-Use Items.” Bundesministerium für Wirtschaft, Energie und Tourismus. Accessed May 29, 2026. <https://www.bmwet.gv.at/en/Topics/Export-Control/Export/Dual-Use.html>.

“(ECCN) and Export Administration Regulation (EAR99).” International Trade Administration | Trade.gov. Accessed May 28, 2026.

<https://www.trade.gov/eccn-and-export-administration-regulation-ear99>.

“End-User and Stockist Undertaking (EUSU) Form Guidance.” GOV.UK. Accessed May 28, 2026.

<https://www.gov.uk/government/publications/end-user-undertaking-euu-form/end-user-undertaking-euu-form-guidance>.

Evidence of U.S. parts in Turkish drones deployed by Azerbaijan. Accessed May 28, 2026.

https://anca.org/assets/pdf/BayraktarDrone_US_Nato_Technology.pdf.

“The Export Control Order 2008.” Legislation.gov.uk. Accessed May 28, 2026.

<https://www.legislation.gov.uk/ukxi/2008/3231/schedule/2/made/data.html>.

“Export Controls: Dual-Use Items, Software and Technology, Goods for Torture and Radioactive Sources.” GOV.UK. Accessed May 28, 2026.

<https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources>.

“Export Controls: Military Goods, Software and Technology.” GOV.UK. Accessed May 28, 2026.

<https://www.gov.uk/guidance/export-controls-military-goods-software-and-technology>.

“Extraterritorial Applications in Export Controls: EU, UK, US, and Cn – What to Consider.”

Export controls EU, UK, US, CN: Extraterritoriality aspects. Accessed May 28, 2026.

<https://www.aeb.com/en/magazine/articles/extraterritoriality-export-controls-us-uk-eu-cn.php#uk>.

Frontline report: Ukraine Strikes Deep into Russia's "untouchable" Caspian Sea, disabling oil platforms and military barges - euromaidan press. Accessed May 28, 2026.

<https://euromaidanpress.com/2025/12/23/frontline-report-2025-12-23/>.

Ghazarian, Matthew. "Drone Empires: Ethnic Conflict, Techno-Spectacle, and Imperial Machinations Across Eurasia and Africa ." Duke University Press, December 1, 2025.

<https://doi.org/10.1215/1089201X-12113388>.

"Guidance on End-User and End-Use Controls and U.S. Person Controls." Bureau of Industry and Security. Accessed May 28, 2026.

<https://www.bis.gov/licensing/guidance-on-end-user-and-end-use-controls-and-us-person-controls>.

"HC 1090 Towards the next Defence and Security Review." parliament.uk. Accessed May 28, 2026.

<https://publications.parliament.uk/pa/cm201314/cmselect/cmdfence/writetv/1090/m04.htm>.

"How the United Kingdom Approaches Export Controls." Global Investigations Review. Accessed May 28, 2026.

<https://globalinvestigationsreview.com/guide/the-guide-sanctions/sixth-edition/article/how-the-united-kingdom-approaches-export-controls>.

"HS-Code List." The Dollar Business. Accessed May 28, 2026.

<https://in.thedollarbusiness.com/hs-codes/electronic-integrated-circuits-processors-controllers/section-16/chapter-854231>.

"Infrared Imaging Solutions for UAVs, UGVs and Unmanned Systems." Lynred. Accessed May 28, 2026. <https://www.lynred.com/UxS-market>.

International Trade Administration. "United Kingdom - Aerospace and Defense." International Trade Administration | Trade.gov, October 5, 2020.

<https://www.trade.gov/country-commercial-guides/united-kingdom-aerospace-and-defense>.

Koren, Kate, and Philip Luck. “Delays and Uncertainty in the Export Licensing Process: Findings from a CSIS Survey of U.S. Technology Exporters.” CSIS. Accessed May 28, 2026.

<https://www.csis.org/analysis/delays-and-uncertainty-export-licensing-process-findings-csis-survey-us-technology>.

Kupemba, Danai Nesta. “British Parts Found in Russian Drones, Zelesnky Says.” BBC News, October 6, 2025. <https://www.bbc.com/news/articles/cg5e9zlpz6eo>.

List of dual-use goods and technologies and munitions list. Accessed May 28, 2026.

<https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf>.

Maria Zholobova (IStories), Benjamin Bidder (Der Spiegel). “Kazakhstan Has Become a Pathway for the Supply of Russia’s War Machine. Here’s How It Works.” OCCRP, May 7, 2026.

<https://www.occrp.org/en/investigation/kazakhstan-has-become-a-pathway-for-the-supply-of-russias-war-machine-heres-how-it-works>.

McEVOY, JOHN. “Israel’s Killer Drones Powered with UK Engines.” Declassified UK, April 28, 2025. <https://www.declassifieduk.org/israels-killer-drones-powered-with-uk-engines/>.

“Military End-Use Controls.” GOV.UK. Accessed May 28, 2026.

<https://www.gov.uk/guidance/military-end-use-controls>.

Morris, Jamie. “Dorset MP Seeks Clarity over Arms Exports to Israel.” BBC News, June 5, 2025.

<https://www.bbc.com/news/articles/cg5v1ljy6ngo>.

“New EU Dual-Use Regulation Increases Focus on Internal Compliance Programmes.” Taylor Wessing, September 2, 2024.

<https://www.taylorwessing.com/en/insights-and-events/insights/2021/09/neue-eu-dual-use-verordnung-erhoeht-den-fokus-auf-interne-compliance-programme>.

Overton, Iain. “Exporting Risk: How UK Arms Sales Overlap with Countries Using Explosive Weapons in Populated Areas.” AOAV, July 20, 2025.

<https://aoav.org.uk/2025/exporting-risk-how-uk-arms-sales-overlap-with-countries-using-explosive-weapons-in-populated-areas/>.

Regulation (EU) 2021/821 - EUR-lex. Accessed May 29, 2026.

<https://eur-lex.europa.eu/eli/reg/2021/821/oj>.

Regulation - 2021/821 - en - EUR-lex. Accessed May 28, 2026.

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0821>.

“Revealed: How British Engines Ended up in Israeli Drones.” Declassified UK, December 11, 2025.

<https://www.declassifieduk.org/revealed-how-british-engines-ended-up-in-israeli-drones/>.

Sofuoglu, Murat. “TRT World - Will Turkey’s Drone Industry Be Affected by UK Firm’s Cut in Exports?” TRT World - Breaking News, Live Coverage, Opinions and Videos, May 3, 2023.

<https://www.trtworld.com/magazine/will-turkey-s-drone-industry-be-affected-by-uk-firm-s-cut-in-exports-43292>.

Stocker, Tom. “UK Signals Increased Export Control Enforcement and Penalties.” Pinsent Masons, December 5, 2025.

<https://www.pinsentmasons.com/out-law/analysis/uk-increased-export-control-enforcement-penalties>.

“UK Export Controls.” Global Sanctions, December 16, 2025.

<https://globalsanctions.com/sanctioning-states/uk/export-controls-3/>.

“UK Sanctions Guidance for Non-UK Businesses.” GOV.UK. Accessed May 28, 2026.

<https://www.gov.uk/guidance/uk-sanctions-guidance-for-non-uk-businesses>.

“UK Strategic Export Controls.” GOV.UK. Accessed May 28, 2026.

<https://www.gov.uk/guidance/uk-strategic-export-controls>.

Ukraine races to make more war drone components at home | reuters. Accessed May 28, 2026.

<https://jp.reuters.com/article/world/ukraine-races-to-make-more-war-drone-components-at-home-idUSKBN3190HC/>.

Ukraine’s Zelenskyy says western parts found in Russian drones, missiles | Russia-Ukraine War News | Al Jazeera. Accessed May 28, 2026.

<https://www.aljazeera.com/news/2025/10/6/ukraine-zelenskyy-says-western-parts-found-in-russian-drones-missiles>.

“Unmanned Air Systems: Question for Department for Business and Trade.” UK Parliament, May 14, 2025.

<https://questions-statements.parliament.uk/written-questions/detail/2025-05-14/52328>.

US targets Chinese companies over drone components used by Hamas, Houthis | Reuters. Accessed May 28, 2026.

<https://www.reuters.com/world/asia-pacific/us-targets-chinese-companies-over-drone-components-used-by-hamas-houthis-2025-10-08/>.

“What Is a Drone Flight Controller?” Grepow. Accessed May 28, 2026.

<https://www.grepow.com/blog/what-is-a-drone-flight-controller.html>.

“Winston Pocket Guide to EU Export Control and Regulation.” Winston & Strawn. Accessed May 29, 2026.

<https://www.winston.com/en/blogs-and-podcasts/european-regulatory-compass/winston-pocket-guide-to-eu-export-control-and-regulation>.

“[Withdrawn] UK Arms Embargo on Armenia and Azerbaijan.” GOV.UK, July 2, 2025.

<https://www.gov.uk/guidance/uk-arms-embargo-on-armenia-and-azerbaijan>.