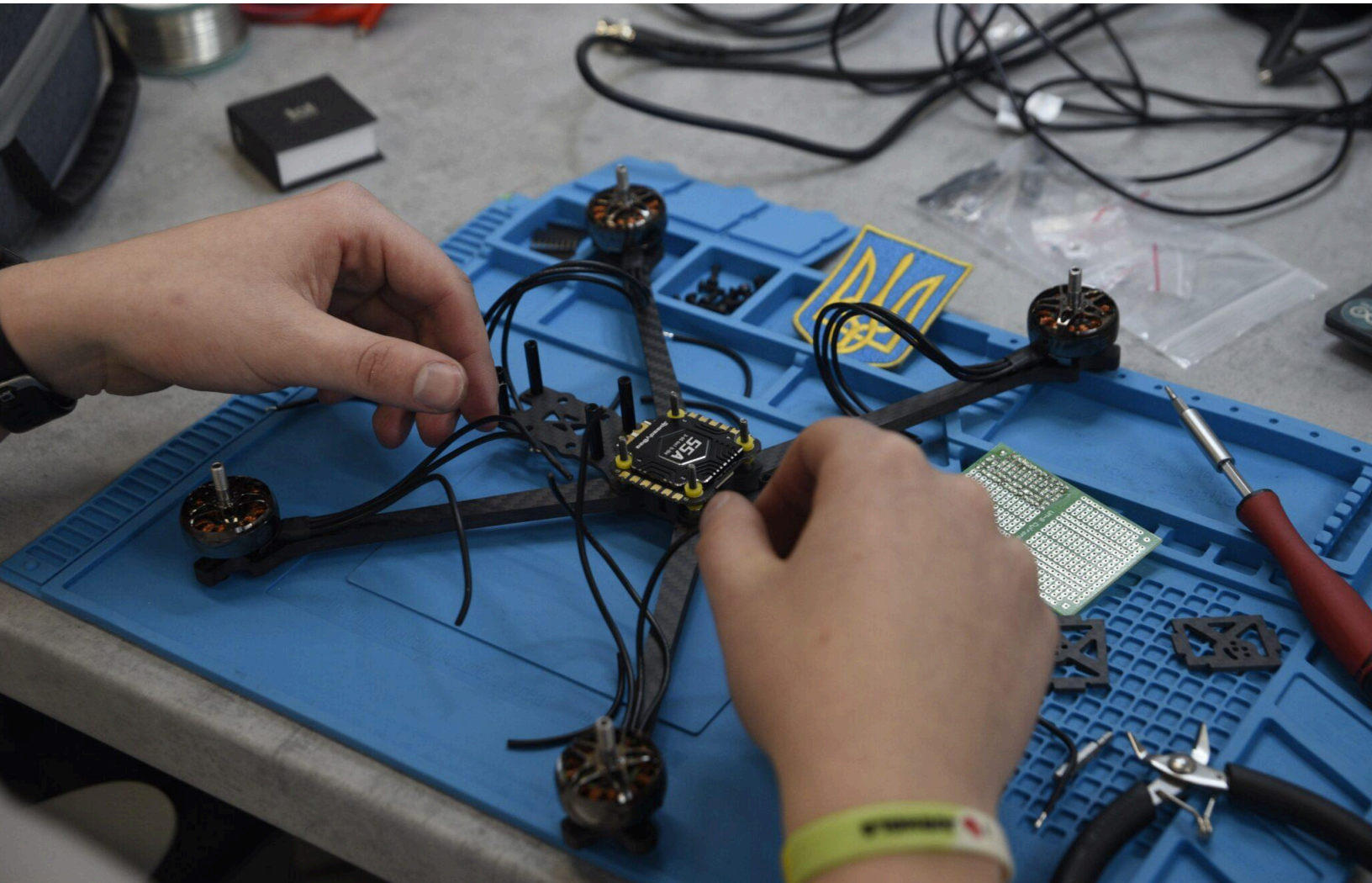
January 16th, 2026

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 **25** 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

The United Kingdom is focused on expanding its drone-industrial base as an economic and defence priority, yet the country's 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 by rendering many off-the-shelf electronic components critical to FPV production.

This paper argues that the issue is primarily structural, and not enforcement-driven. The UK's export control legal framework permits components that are functionally capable for integration into military drones to be exported 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 enabling diversion and re-export, and documentation practices that stress benign end uses. The paper then grounds these mechanisms through three case studies of UK-origin components appearing in drones utilized in conflict-zones, with each examining the relevant loophole that enabled each instance to occur. Comparative case studies of the US and EU export control regimes follow this to determine the structural features contributing 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

The government of the United Kingdom, as part of its Defense Industrial Strategy, positions drones and related technologies as a pillar of a broader effort to use defense as an engine of economic growth, supported by state investment and skills programs.[1] By 2030, the UK drone manufacturing industry is projected to contribute up to £30 billion to the national economy, reflecting rapid expansion across both civilian and defense applications.[2] Unlike other producers, which focus on complete drone platforms, the UK's comparative strength lies in high-value subsystems, such as micro-electromechanical system (MEMS) sensors, navigation systems, optical sensors, and lightweight composite airframes.[3]

UK-made 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.[4] Flight-control microcomputers produced by UK firms have broad recreational and civilian applications, but have also been found in first-person view (FPV) drones throughout the Russo-Ukrainian War.[5] These are just two examples of drone components that have both civilian and military applications; yet it becomes clear that drone subsystems traditionally used in only civilian contexts are now inherently dual-use.

The UK drone subsystem industry has experienced sustained export growth over the past decade, especially to states that serve as intermediaries in global drone supply chains, such as Israel, Saudi Arabia, Turkey, and the UAE.[6] UK Arms export data illustrates the broader context: between 2021 and 2024, the UK authorized between £1 billion and £4.5 billion per year in arms and related licences to 84 countries, 23 of which used explosive weapons in populated areas, causing tens of thousands of civilian deaths and injuries. Saudi Arabia, Turkey, and the UAE remain among the key customers. UK-origin technology and components have supported foreign drone programmes such as Turkey's Bayraktar series and Israeli drones implicated in explosive violence against civilians.[7]

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.[8] Although all drone components should be subject to dual-use licensing, the present regulatory system allows a significant quantity to be exported as uncontrolled goods—requiring no license and commercially available. However, these same uncontrolled components have been documented in drones found in Gaza, Nagorno-Karabakh, and Ukraine. While these components are often used for civilian purposes, it is critical that they be subject to a dual-use licensing schedule, as they can easily be repurposed into conflict-zone-capable drones.

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 licences, complete end-use verification checks, and maintain extensive audit-ready documentation.[2] Firms often avoid this designation because it slows export timelines significantly and can block access to certain markets. Overall, dual-use status increases compliance costs, introduces liability risk, and can trigger customer concerns in non-defense commercial sectors.

Since the early 2010s, drone-manufacturing firms have engaged in behavior such as slightly modifying their products to classify them on less stringent controlled-goods lists.[10] However, evading licensing entirely is a relatively new issue that coincides with the rise of modern warfare using FPV drones manufactured with traditionally off-the-shelf technology. Advocacy organizations have released explicit evidence of UK-made drone components implicated in explosive violence against citizens that were exported as uncontrolled goods. However, in response to findings that drone components were found in Russian drones, the UK Government responded that "it is making every effort to stop British companies from exporting components for weapons production to Russia," but would look into the issue nonetheless.[11] This response highlights that the UK Government did not have prior knowledge of the extent of the issue and is reactively acting to violations of export controls. A significant motivating factor for the lack of government action is industry lobbying from UK defense companies, which have consistently campaigned to either remove licensing requirements for drones and drone components since 2011.[12]

Regulatory Framework and Gaps

This section analyzes the structural legal framework of the UK export control regime to reveal two regulatory gaps that enable drone components with inherent dual-use functions to avoid licensing requirements.

Performance-based Thresholds

A major initial structural gap stems from the emphasis placed on performance-based thresholds in the Strategic Export Control List, which allows goods with the functional capability to integrate into military drones to be exported uncontrolled, so long as 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.[14] These categories control components only when they exceed specific performance levels.[15] This use of performance-based thresholds was an intentional design choice originally intended to avoid over-regulating mass-market commercial electronics in a technological context where strategically sensitive hardware was clearly distinguishable from commercial electronics.[16]

However, with the rise of drone warfare, FPV drones are often constructed out of the same components that a drone hobbyist could purchase online, which fall far below the Strategic Export Control List's performance thresholds.[17] Presently, a more important metric is function: two components can have the same capability to be integrated into a military drone with only a tiny difference in performance, but one would be controlled, and the other would not. The present threshold-based model is outdated and excludes many commercially available components used in FPV drones, including optical sensors, microcontrollers, and avionics subsystems, because they fall below the established performance requirements. As a result, these items are legally permitted for export to countries of concern. This dynamic reflects a structural issue of the export-control system rather than an enforcement failure. Firms could exploit the system by slightly decreasing the performance of their goods to ensure they can be exported on uncontrolled schedules. Although there is currently no evidence of wrongdoing, UK arms companies have abused performance-based thresholds in the past by slightly decreasing the performance of their products.[18]

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, there is far less oversight of uncontrolled goods.[19] To prevent uncontrolled goods from being used 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.[20] 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 as "No License Required," (NLR) there is little oversight of the export's destination and purpose.[21] 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 undertake measures to hide the extent of their knowledge of downstream buyers and their purposes and consciously forgo applying for a license even when they are legally required. Given that this system of catch-all controls creates a payoff structure in which the benefits of an expedited process and saved costs far outweigh the low likelihood of being caught, it is a rational decision for firms to evade the UK catch-all controls. As a result of the emphasis on firms to self-classify, the catch-all mechanism captures only a narrow subset of UAV-capable components that fall below control thresholds but nonetheless contribute to military drone manufacturing.

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 them from violating 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 weak and fragmented enforcement capacity has created an environment in which firms are likely to violate catch-all controls, hide their tracks, and maintain plausible deniability if caught. 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 uncontrolled goods shipments only when exporters voluntarily seek a licence or request guidance.[24] 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.[25] Critically, when firms are caught violating catch-all controls, criminal prosecution requires proof of conscious intent to subvert catch-all controls. This subjective threshold has incentivized exporters to characterize violations of catch-all controls as accidental errors.[26] In 2023, HMRC and Border Force reported 266 seizures of misclassified goods and 260 voluntary disclosures, yet secured only 15 criminal prosecutions.[27] This data reveals that British firms are using a variety of methods to evade being caught for violating catch-all controls and to feign innocence if caught.[28]

Harmonized System

To evade detection for violating catch-all controls, exporters frequently take advantage of the Harmonized System (HS), a globally standardized system for classifying goods, to shape how HMRC perceives their goods. However, by categorizing goods according to broad physical characteristics, HS codes compound the opaqueness of exports. Exporters often select classifications that make uncontrolled drone components with potential military applications appear benign, reducing the likelihood of scrutiny.[29]

HS code 8542.31 illustrates this problem. This umbrella category encompasses both low-value consumer microcontrollers and the high-performance processors that have been recovered from Russian guidance systems.[30] 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 ubiquitous in civilian electronics, it continues to be treated as a standard commercial code at the border.[31] 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.[32]

End-use verification & Re-exporting

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 Licence (SIEL), they must submit an End-User Undertaking (EUU) form to identify the final user.[33] However, uncontrolled shipments do not require an EUU. 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 for being associated 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.[34] 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 fill out an EUU, 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 profit. Regardless, the UK has still not integrated these shortcomings into updated procedures: shipments through known transshipment hubs do not automatically trigger ECJU review or enhance due diligence by HMRC.

Secondly, on invoices, audits, and other documents tracking exports, firms will emphasize the final commercial uses of the export. Compliant intermediary firms will be told to stress benign purposes for the imports in export documents, such as agricultural surveying or industrial monitoring. These descriptions satisfy formal documentation and make it difficult for HMRC to demonstrate the requisite knowledge threshold for prosecution.

Recap

In conclusion, a combination of the ECJU putting the onus to self-classify on firms themselves and a lack of required documentation results in a weak oversight framework that incentivizes firms to carefully evade the requirements of catch-all controls. Firms 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 conviction of knowingly violating catch-all controls nearly impossible.

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 lays out three illustrative case studies of uncontrolled UK-made drone components appearing in conflict zones and analyzes the legal and enforcement deficiencies allowing each instance to occur.

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.[35] UK authorities stated that no export licenses had been granted to Azerbaijan, which had been under an arms embargo since 1992.[36] Given that Azerbaijan was under an arms embargo, the most likely explanation of how UK-made drone components ended up used by the Azerbaijani military is that the components were integrated into drones and then re-exported.

Andair confirmed that it was exporting its components to Baykar, the manufacturer of the TB2 drone.[37] Andair's fuel valve is below the thresholds outlined in the Strategic Export Control List, but as Baykar is a defense company, it is highly unlikely that Andair was able to evade catch-all controls and presumably obtained a SIEL. However, once incorporated into TB2's, these products were re-exported to Azerbaijan without the knowledge of UK authorities. When the case was broken, Andair terminated its relationship with Baykar to comply with UK export controls.[38]

The knowledge gap of UK authorities is driven by the weak end-user certification methods contained in SIELs. SIELs only require pre-export end-user certification measures, such as EUUs, yet have no post-export end-user certification measures, such as PSV checks.[39] The Andair fuel valve case thus reveals a deeper issue with the UK's export control regime: inadequate end-user certification measures in SIELs allow intermediary nations to incorporate UK drone components, then re-export them to sanctioned entities outside of UK oversight. The UK must either reform SIELs to incorporate stronger end-user certification measures or strengthen catch-all controls to require a more stringent license to be obtained. While it is unknown whether Andair was aware of the re-export of their components, UK authorities were certainly unaware until the watchdog report was revealed.[40]

Case Study Two: Interpretive Decontrol

In 2024, investigative reporting revealed that Israeli Aerospace Industries' APUS-25 quadcopter, which has been used in Gaza strikes, was equipped with heavy-fuel engines produced by Dorset-based RCV Engines.[41] 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.[42] 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.[43] 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 interpreted as falling below the "specially designed for military use" threshold, allowing RCV to export them under commercial channels or Open General Export Licenses without SIELs or end-user certification.[44]

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.[45] Even after the UK suspended around thirty export licences to Israel in late 2024, RCV's products continued to move freely, unaffected by the broader restrictions.[46] Campaign groups have argued that this regulatory gap, reinforced by political lobbying and influence within the arms lobby in Parliament, created a structural exemption that enabled UK-made drone engines to enter an active conflict zone with no oversight.[47] 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 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 night of October 5th, 2025, Russia used 549 weapons containing 102,785 foreign-made components, including UAVs with UK-made avionics and microcontrollers.[48] 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," but would look into the issue nonetheless.[49]

Investigations into Russian Orion, Shahed-variant, and Lancet UAVs repeatedly show that once sold to third-country clients, such as Armenia, Kazakhstan, Kyrgyzstan, and the UAE, such components are re-exported

into Russia's drone programme without triggering UK oversight.[50] For example, Kazakhstan's exports of microchips to Russia jumped from $245,000 in 2021 to $18 million in 2022, demonstrating the exponential increase in re-exports to Russia.[51]

This case highlights several issues with the UK export control regime. These avionics and microcontrollers are functionally capable of integration into UAVs 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 catch-all controls, requiring a license only if there is reason to suspect the product will be used for military purposes under catch-all controls. By utilizing intermediary countries and exporting under traditionally commercial HS codes, firms 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 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 the massive increase in re-exports of drone components to Russia as firms are incentivized to evade catch-all controls through intermediary firms and ambiguous HS codes while maintaining plausible deniability if caught.

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 uncontrolled 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).[52]

The US system is characterized by a combination of list-based controls, broad catch-all rules, stringent end-user screening, extraterritorial jurisdiction, and strong enforcement infrastructure. Together, these features enable the US to regulate civilian-classified drone components more aggressively than many other countries. The US system is widely regarded as one of the most comprehensive and strongly enforced export control regimes globally, particularly in its treatment of civilian-classified but militarily sensitive technologies.[53]

Classification

Items subject to US export controls are classified under the Commerce Control List (CCL) through an Export Control Classification Number (ECCN).[54] Many advanced drone components, including specialized sensors, guidance electronics, and avionics, fall under specific ECCNs and require export licences prior to shipment. This list-based classification system provides the primary technical foundation of US export controls.

Within the CCL framework, "normal commercial items" fall under the generic classification EAR99. This category includes many components that may be used in drones but are not designated as "military-grade," such as inertial sensors, imaging modules, GNSS receivers, and MEMS components. This ensures that civilian-classified components are not automatically exempt from scrutiny.[55]

While the UK maintains a dual-use list, uncontrolled electronics that do not meet performance thresholds fall under "non-listed items" and are subject only to UK catch-all controls. However, UK catch-all controls are narrower and applied less frequently than US EAR99 scrutiny. In practice, if an item is uncontrolled, UK exporters often assume

it is low-risk unless explicitly notified otherwise by authorities. Thus, the conceptual structure exists in the UK, but the operational use is far less expansive than EAR99.[56]

EAR Part 744 Catch-All Controls

The US maintains one of the broadest catch-all systems in the world. The EAR focuses on end-user-based controls, under which controlled or EAR99 goods are automatically subject to licensing requirements if the importer is on the Entity List, Military End-User List, or Denied Persons List.[57] This objective system, focusing on who the buyer is, removes any question of whether the exporter had reasonable grounds to suspect military use. For drone components, this is crucial because commercial electronics are widely substitutable in military UAVs.[58]

In contrast, the UK catch-all controls focus on whether firms have reasonable grounds to suspect that their goods will be used for military purposes. If a firm's goods are found in foreign military products, authorities must prove that the firm had the requisite knowledge of the final use of their goods, which is subjective and easy to contest. As maintaining plausible deniability is easy when found violating catch-all controls, firms are incentivized to evade them. Given that the burden of detecting suspicious end-use is primarily on the firm rather than on the government, as in the US system, evasion is incentivized.

End-User Lists and Beneficial Ownership Screening

Under US catch-all controls, if the end-user is a known high-risk or sanctioned entity, even "harmless" parts require an export license. BIS maintains the Entity List, along with related control lists such as the Denied Persons List, Unverified List, and Military End-User List. These lists identify organizations and firms considered high-risk.[59] If an export involves any listed party, including the purchaser or end-user, a licence is required, even for EAR99 civilian items, as part of US catch-all controls. As of 2025, BIS also applies a 50% beneficial ownership rule, treating any foreign company owned or controlled by a listed entity as if it were itself listed.[60] This broadens the web of scrutiny across international supply chains.

The UK maintains its own lists (e.g., the UK Sanctions List, Military End-Use controls). However, the UK does not employ a 50% ownership rule, and its sanctions listings are narrower than those on the US Entity List. Thus, the UK system is less expansive in scope, and beneficial-ownership-based screening is not present in a comparable form.

De Minimis Extraterritorial Rule

The US applies a de minimis jurisdiction rule under the EAR, 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.[61] 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.

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. Thus, this powerful US regulatory tool has no UK parallel.

Enforcement and Post-Shipment Verification

The BIS conducts PSV checks abroad for both controlled items and civilian-classified EAR99 items when a diversion risk exists. Triggers for PSV for uncontrolled items include suspicious intermediaries, newly formed trading companies, high-risk destinations, and links to sanctioned entities or military drone programs.[62] Moreover, the BIS operates a formal overseas end-use monitoring program, under which US officials visit foreign buyers after export. BIS further monitors re-export pathways using end-use checks, intelligence reports, and battlefield component recovery.[63] These PSV checks create a credible deterrent and enable detection of actual diversion into military UAV supply chains.

On the other hand, the UK does not conduct any sort of PSV checks to monitor the end-use of military and dual-use equipment exported from the UK.[64]

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.[65] 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.[66] 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.[67] 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.

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.[68] 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 the 2021 recast.[69] UK authorities rely more heavily on case-by-case notifications, unlike the EU framework's broader "know or suspect" standard. Thus, UK authority technically exists but is less active, less expansive, and less risk-based.

Article 5 (Cyber-Surveillance Catch-All)

The EU has a unique provision allowing restrictions on non-listed cyber-surveillance tools that could be used for human-rights violations. This 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 drone-surveillance items. Thus, this is a significant regulatory difference.

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.[70] This law shifts part of the responsibility for risk assessment to the private sector, improving early detection of problematic end users.[71]

The UK encourages compliance programs but does not require them. 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.

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 in military FPV drones highlight the need for function-based controls. The UK could model this system off 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. In particular, the UK should implement a 50% ownership rule modeled off the US system, which treats any foreign company owned or controlled by a listed entity as if it were itself listed.
- **Third,** the UK should reform its **catch-all controls** to require that any goods exported to a listed entity obtain a license. 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 Licences** which require less end-user certification, for drones, drone components, and related software, requiring instead 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.[72] In 2024, the Committees on Arms Export Control was disbanded and replaced with a far smaller sub-committee within the Business and Trade Committee.[73]
- **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.

Endnotes

1. Export Control Joint Unit, "Export Controls: Dual-Use Items, Software and Technology, Goods for Torture and Radioactive Sources," *GOV.UK*, 2019, https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources.
2. Fortune Business Insights, "Drone Payload Market Size, Share, Trends, Forecast, 2034," *Fortune Business Insights*, 2025, https://www.fortunebusinessinsights.com/drone-payload-market-113108.
3. Strategic Trade Research Institute, *Position, Navigation, and Timing: A Sectoral Composition Approach* (College Park, MD: Strategic Trade Research Institute and Center for International and Security Studies at Maryland, October 2020).
4. "FPV Drone Components," Scribd document, uploaded by darwishrsi, accessed January 14, 2026, https://www.scribd.com/document/888366416/FPV-Drone-Components.
5. Kateryna Shkarlat, "UK Reacts to Zelenskyy's Statement about Its Components in Russian Drones and Missiles," *RBC-Ukraine*, October 6, 2025, https://newsukraine.rbc.ua/news/uk-reacts-to-zelenskyy-s-statement-about-1759768390.html.
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. Ibid.
8. Parliament of the United Kingdom of Great Britain and Northern Ireland, "The Export Control Order 2008," *legislation.gov.uk*, December 15, 2008, https://www.legislation.gov.uk/uksi/2008/3231/made.
9. ECJU, "Export Controls: Dual-Use Items…
10. James Rogers, "Written Evidence on the Domestic Threat of Drones," evidence submitted to the All-Party Parliamentary Group on Drones, UK Parliament Committees, accessed January 14, 2026, https://committees.parliament.uk/writtenevidence/103872/html/.
11. Shkarlat, "UK Reacts to Zelenskyy's Statement"; "British Parts Found in Russian Drones Attacking Ukraine amid Calls for Tighter Sanctions," *NationalWorld*, October 6, 2025, accessed January 14, 2026, https://www.nationalworld.com/news/british-parts-found-in-russian-drones-attacking-ukraine-amid-calls-for-tighter-sanctions-5347811.
12. Chris Cole, "Industry Lobbying to Change Drone Export Control Rules," *Drone Wars UK*, November 28, 2011, https://dronewars.net/2011/11/28/industry-lobbying-to-change-drone-export-control-rules/.
13. Wassenaar Arrangement Secretariat, *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies: Volume II—List of Dual-Use Goods and Technologies and Munitions List* (2023), https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf.
14. "Control Lists," *The Wassenaar Arrangement*, December 8, 2025, https://www.wassenaar.org/control-lists/.
15. Ibid.
16. Farah Sonde, "Fact Sheet: The Wassenaar Arrangement," *Center for Arms Control and Non-Proliferation*, March 13, 2023, https://armscontrolcenter.org/fact-sheet-the-wassenaar-arrangement/.
17. Dmytro Sazonov, "How to Build an FPV Combat Drone for Military Purposes," *Medium* (Illumination Curated), April 18, 2025, accessed January 14, 2026, https://medium.com/illumination-curated/how-to-build-an-fpv-combat-drone-for-military-purposes-ce549f24efca.
18. House of Commons, "Written Evidence on Quadrennial Defence Review 2013," UK Parliament (House of Commons), publication page, https://publications.parliament.uk/pa/cm201314/cmselect/cmdfence/writev/1090/m04.htm.
19. HM Revenue & Customs, "About Us," *GOV.UK*, accessed January 14, 2026, https://www.gov.uk/government/organisations/hm-revenue-customs/about.
20. United Kingdom, "End-use Controls Applying to Military-related Items," *GOV.UK* guidance, accessed January 14, 2026, https://www.gov.uk/guidance/end-use-controls-applying-to-military-related-items; One critical conclusion of this is that it is entirely illegal for a firm to export an uncontrolled good without obtaining a license if there is reasonable suspicion it will be used for military purposes.
21. Ibid.
22. Sonde, "Fact Sheet: The Wassenaar Arrangement."
23. Sazonov, "How to Build an FPV Combat Drone for Military Purposes."
24. Raminta Dereskeviciute, Ludovica Rabitti, and Michal Chajdukowski, "How the United Kingdom Approaches Export Controls," *Global Investigations Review*, June 30, 2025,

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

25. HM Revenue & Customs, "About Us."
26. Foreign, Commonwealth & Development Office and Office of Financial Sanctions Implementation, "UK Sanctions Guidance for Non-UK Businesses," *GOV.UK*, last modified November 27, 2025, https://www.gov.uk/guidance/uk-sanctions-guidance-for-non-uk-businesses.
27. Dereskeviciute, Rabitti, and Chajdukowski, "How the United Kingdom Approaches Export Controls."
28. 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.
29. Maya Lester KC and Michael O'Kane, "UK Export Controls," *Global Sanctions*, accessed December 23, 2025, https://globalsanctions.com/sanctioning-states/uk/export-controls-3/; Export Control Joint Unit and Department for Business and Trade, "Export Controls: Dual-Use Items, Software and Technology, Goods for Torture and Radioactive Sources," *GOV.UK*, last modified April 2, 2025, https://www.gov.uk/guidance/export-controls-dual-use-items-software-and-technology-goods-for-torture-and-radioactive-sources.
30. "HS Code of 854231 (Electronic Integrated Circuits: Processors and Controllers, Whether or Not Combined With Memories, Converters, Logic Circuits, Amplifiers, Clock and Timing Circuits, or Other Circuits)," *The Dollar Business*, accessed December 23, 2025, https://in.thedollarbusiness.com/hs-codes/import/854231/electronic-integrated-circuits-processors-controllers; United Nations Statistics Division, "HS, 2012—Code 854231," accessed December 23, 2025, https://unstats.un.org/unsd/classifications/Econ/Detail/EN/32/854231.
31. U.S. Department of Commerce, Bureau of Industry and Security, "Common High Priority Items List (CHPL)," accessed January 14, 2026, https://www.bis.gov/licensing/country-guidance/common-high-priority-items-list-chpl.
32. *Export Control Joint Unit, "Export Controls: Dual-Use Items, Software and Technology, Goods for Torture and Radioactive Sources."*
33. Export Control Joint Unit and Department for Business and Trade, "End-user and Stockist Undertaking (EUSU) Form Guidance," *GOV.UK*, last modified September 8, 2025, https://www.gov.uk/government/publications/end-user-undertaking-euu-form/end-user-undertaking-euu-form-guidance.
34. "UK Engines Powered Israeli Drones Used in India–Pakistan Conflict, Reports Say," *Middle East Eye*, published May 18, 2025, accessed January 14, 2026, https://www.middleeasteye.net/news/uk-engines-powered-israeli-drones-used-india-pakistan-reports-say; "Frontline Report: Kazakhstan Cuts Off Key Supply Route for Russia's War Machine with New Export Controls," *Euromaidan Press*, December 23, 2025, accessed January 14, 2026, https://euromaidanpress.com/2025/12/23/frontline-report-2025-12-23-2a/.
35. "New Evidence Reveals Six-Year History of UK Supplies to Turkish Killer Drones," *Freedom News*, January 15, 2021, https://freedomnews.org.uk/2021/01/15/new-evidence-reveals-six-year-history-of-uk-supplies-to-turkish-killer-drones/.
36. "Bayraktar TB2," *Drone Warfare Center* (Warbirds Resource Group), accessed January 2026, https://dronewarfarecenter.com/dwc-air-bayraktar_tb2.html.
37. CivilNetTV (@CivilNetTV), "British Andair Ltd manufacturerer of fuel system items has stopped supplying its components for #Turkish Bayraktars," *X* (formerly Twitter), January 13, 2021, https://x.com/CivilNetTV/status/1349243020592508930.
38. CivilNetTV (@CivilNetTV), "British Andair Ltd manufacturerer…," *X* (formerly Twitter), January 13, 2021, https://x.com/CivilNetTV/status/1349243020592508930.
39. United Kingdom, "Notice to Exporters 2025/20: Updated End-User Undertaking (EUU) and Guidance," *GOV.UK*, May 20, 2025, https://www.gov.uk/government/publications/notice-to-exporters-202520-updated-end-user-undertaking-euu-and-guidance/nte-202520-updated-end-user-undertaking-euu-and-guidance; House of Commons Library, *UK Arms Exports and Export Control Policies: Research Briefing* (January 24, 2024), 6, https://researchbriefings.files.parliament.uk/documents/CBP-8312/CBP-8312.pdf.
40. "Bayraktar TB2," *Drone Warfare Center.*
41. 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.
42. Ibid.
43. "Question for Department for Business and Trade," UK Parliament, May 14, 2025, https://questions-statements.parliament.uk/written-questions/detail/2025-05-14/52328.
44. House of Commons Library, *UK Arms Exports and Export Control Policies*, 6.
45. Ibid.
46. Ibid.
47. Ibid.

48. Shkarlat, "UK Reacts to Zelenskyy's Statement about Its Components in Russian Drones and Missiles"; Al Jazeera Staff, "Ukraine: Zelenskyy Says Western Parts Found in Russian Drones and Missiles," *Al Jazeera*, October 6, 2025, https://www.aljazeera.com/news/2025/10/6/ukraine-zelenskyy-says-western-parts-found-in-russian-drones-missiles.
49. Shkarlat, "UK Reacts to Zelenskyy's Statement about Its Components in Russian Drones and Missiles"; https://newsukraine.rbc.ua/news/uk-reacts-to-zelenskyy-s-statement-about-1759768390.html; "British Parts Found in Russian Drones Attacking Ukraine amid Calls for Tighter Sanctions," accessed January 14, 2026.
50. "Kazakhstan Has Become a Pathway for the Supply of Russia's War Machine—Here's How It Works," *Organized Crime and Corruption Reporting Project (OCCRP)*, December 23, 2025, accessed January 14, 2026, https://www.occrp.org/en/investigation/kazakhstan-has-become-a-pathway-for-the-supply-of-russias-war-machine-heres-how-it-works.
51. "Frontline Report: Kazakhstan Cuts Off Key Supply Route for Russia's War Machine with New Export Controls," *Euromaidan Press*, December 23, 2025, accessed January 14, 2026, https://euromaidanpress.com/2025/12/23/frontline-report-2025-12-23-2a/.
52. Bureau of Industry and Security, "Export Administration Regulations (EAR)," *BIS*, accessed January 14, 2026, https://www.bis.gov/regulations/ear.
53. Martin Chorzempa and Laura von Daniels, "New US Export Controls: Key Policy Choices for Europe: Recommendations for a Robust European Export Control Policy," *SWP Comment* 2023/C 20 (Stiftung Wissenschaft und Politik, March 24, 2023), accessed January 14, 2026, https://www.swp-berlin.org/10.18449/2023C20.
54. Bureau of Industry and Security, "Export Administration Regulations (EAR)," *BIS*, accessed January 14, 2026, https://www.bis.gov/regulations/ear/774.
55. Bureau of Industry and Security, "Export Administration Regulations (EAR), Supplement No. 1 to Part 774—The Commerce Control List," *BIS*, accessed January 14, 2026, https://www.bis.gov/regulations/ear/774#supplement-1-774.
56. Ibid.
57. U.S. Department of Commerce, Bureau of Industry and Security, "15 C.F.R. Part 744—Control Policy: End-User and End-Use Based," *eCFR*, accessed January 14, 2026, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744?toc=1.
58. Bureau of Industry and Security, "Export Administration Regulations (EAR)."
59. Bureau of Industry and Security, "Guidance on End-User and End-Use Controls and U.S. Person Controls," *BIS*, 2025, https://www.bis.gov/licensing/guidance-on-end-user-and-end-use-controls-and-us-person-controls.
60. "Expansion of End-User Controls to Cover Affiliates of Certain Listed Entities," *Federal Register*, September 30, 2025, https://www.federalregister.gov/documents/2025/09/30/2025-19001/expansion-of-end-user-controls-to-cover-affiliates-of-certain-listed-entities.
61. "15 CFR § 734.4—De Minimis U.S. Content," *eCFR*, accessed January 14, 2026, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.4.
62. U.S. Government Accountability Office, *Export Controls: Post-Shipment Verification Provides Limited Assurance That Dual-Use Items Are Being Properly Used* (GAO-04-357) (Washington, DC: GAO, 2004), https://www.gao.gov/products/gao-04-357.
63. Ibid.
64. House of Commons Library, *UK Arms Exports and Export Control Policies: Research Briefing* (January 24, 2024), 6, https://researchbriefings.files.parliament.uk/documents/CBP-8312/CBP-8312.pdf.
65. European Union, "Regulation (EU) 2021/821," *EUR-Lex*, accessed January 14, 2026, https://eur-lex.europa.eu/eli/reg/2021/821/oj.
66. Ibid.
67. Winston & Strawn LLP, "Winston Pocket Guide to EU Export Control and Regulation," *European Regulatory Compass*, 2025, https://www.winston.com/en/blogs-and-podcasts/european-regulatory-compass/winston-pocket-guide-to-eu-export-control-and-regulation.
68. "Dual-Use Items," Bundesministerium für Wirtschaft, Energie und Tourismus, 2021, https://www.bmwet.gv.at/en/Topics/Export-Control/Export/Dual-Use.html.
69. Covington & Burling LLP, "An Overview of the Recast EU Dual Use Regulation," 2023, https://www.cov.com/en/news-and-insights/insights/2021/09/an-overview-of-the-recast-eu-dual-use-regulation.
70. Michael Brüggemann, "New EU Dual-Use Regulation Increases Focus on Internal Compliance Programmes," *Taylor Wessing*, September 6, 2021, https://www.taylorwessing.com/en/insights-and-events/insights/2021/09/neue-eu-dual-use-verordnung-erhoeht-den-fokus-auf-interne-compliance-programme.
71. Raminta Dereskeviciute, "EU Member States Implement Additional Measures to Regulate Export of Non-Listed Dual-Use Items," *The National Law Review*, 2024, https://natlawreview.com/article/eu-member-states-implement-additional-measures-regulate-export-non-listed-dual-use.
72. UK Parliament, "Committees on Arms Export Controls," accessed January 2026, https://committees.parliament.uk/committee/15/committees-on-arms-export-controls/.

73. UK Parliament, "Business and Trade Sub-Committee on Economic Security, Arms and Export Controls: Membership," accessed January 2026, https://committees.parliament.uk/committee/783/business-and-trade-subcommittee-on-economic-security-arms-and-export-controls/membership/.