

COUNTERING DRONE PROLIFERATION FROM RUSSIA'S WAR AGAINST UKRAINE: IMPLICATIONS FOR ARMS CONTROL AND SECURITY GOVERNANCE

DOMINIKA KUNERTOVA

I. INTRODUCTION

This paper starts from the simple observation that a drone wall at Europe's external borders is important but not sufficient to protect Europeans against a full drone threat picture. Drones now allow hostile state and non-state actors to access airspace cheaply and with deliberate ambiguity. They can be used as an instrument of hybrid warfare to spy, intimidate and disrupt without crossing the threshold of conventional armed attack.

In contrast, drone interference at airports, in defence industrial zones and at military sites can create fear and uncertainty if left unattributed. Cheap drone technologies also enable illicit drug trafficking by criminal networks, while drone proliferation empowers non-state armed groups south of the Mediterranean Sea. Taken together, dual-use, low-cost drones pose a complex security threat.

Europe is confronted with a drone dichotomy. On the one hand, there is a clear national security imperative to build Europe's own drone industrial base and deepen cooperation with Ukraine, which has become the most dynamic laboratory for contemporary drone warfare. On the other hand, a series of Russian drone incursions in the autumn of 2025 showed that Europe is struggling to defend itself against hostile drones. The same technologies that European armed forces want to integrate are fuelling a wider threat environment that European countries are not yet in a position to manage. The spillover of drone warfare from Ukraine is therefore not limited to military innovation, doctrinal adaptation or new procurement priorities. How European governments navigate this tension between drone capability building and drone threat reduction has rapidly become a pressing issue.

SUMMARY

European governments now face not only the drone innovation challenge but also a new security threat. Cheap and scalable dual-use drone technologies are spreading across battlefields and borders alike. Violations of sovereign airspace by Russian drones are not isolated incidents. Drones are increasingly disrupting air traffic and commerce, and affecting public confidence, while concerns about drone-enabled crime increase on the European Union's southern borders. This widening spectrum of the drone threat has sounded the alarm in European Union and North Atlantic Treaty Organization (NATO) member states. Russia's war against Ukraine has accelerated the diffusion of drone technologies and their lethal use as gaps in export control mechanisms and opaque supply chains have reduced the barriers to the production of weaponized aerial assets. While a drone wall along NATO's eastern borders is important, a technological solution alone is not sufficient. This paper suggests that the drone threat comes in the form of rapid proliferation, airspace ambiguity and sanctions evasion. How can European countries prevent cheap drone interference from becoming a normalized instrument of pressure against Europe? The paper examines the key issues of dormant arms trade regulations, escalation risks linked to underdeveloped airspace governance and loopholes in dual-use technology export control.

ABOUT THE AUTHOR

Dominika Kunertova is a Research Fellow at the Harvard Kennedy School's Belfer Center for Science and International Affairs, an Affiliate Researcher of Peace Research Center Prague in the Department of Social Sciences at Charles University, and a non-resident Senior Fellow at the Atlantic Council's Transatlantic Security Initiative.

Drones used to raise issues around aviation safety and market opportunities. Today, however, EU policymakers regard drones primarily as a security question. The Readiness Roadmap 2030 includes the European Drone Defence Initiative as one of its flagship projects to highlight a key capability shortfall.¹ The European Commission's February 2026 EU Action Plan on Drone and Counter Drone Security seeks to further drone-proof civilian border and critical infrastructure protection, in addition to the usual goal of boosting European drone production.²

This paper suggests, however, that the drone threat to Europe is not just a cost asymmetry challenge, but also raises escalation and illicit proliferation risks. Despite extensive sanctions, Russia has been able to exploit the lack of cost-effective counter-drone measures and the porous export controls around drone components. Insufficient detection, identification and interception systems and procedures further contribute to false alarms and drone scares, deepening the sense of insecurity among European populations. The speed of illicit drone proliferation and the weaknesses of current regulatory mechanisms amplify the security challenge.

Importantly, Europe's drone problem does not exist in a vacuum. Drone technologies continue to evolve rapidly, but there is little political appetite for stronger controls on their transfer and use. However, the mismatch between technology and regulation continues to grow. While many lethal drones now function more like portable rockets or ammunition, most international standards, including the Arms Trade Treaty and the Missile Technology Control Regime (MTCR), still tend to treat drones as potent long-range delivery platforms. The current lack of terminological clarity creates confusion for policymakers, complicates export control practice and blurs the line between systems that demand different forms of regulation and monitoring.

This paper examines the spillover effects of Russia's war against Ukraine. Section II traces the character and scope of the drone threat facing Europe along the eastern and southern vectors. It outlines its layered character in the form of Russian cross-border drone incursions, localized drone disruptions and organized criminal drone activity.

Section III identifies recent drone developments in terms of technology, operations and tactics to highlight the broader security governance implications. These include rapid proliferation of new lethal drones with no accurate transfer data, cost asymmetry and ambiguity that disadvantage the defender and sanctions evasion linked to opaque dual-use technology supply chains.

Section IV details policy recommendations. They follow from analysing how these negative trends raise three key issues of relevance to technology governance, non-proliferation and disarmament: dormant arms trade regulations, increased escalation risks and illicit drone proliferation.

The paper concludes with proposing the ways forward for the European Union and European governments. Existing governance mechanisms were built for an earlier generation of drones. They are poorly adapted to the proliferation of low-cost, dual-use, scalable drone ecosystems that has been accelerated by Russia's war against Ukraine. The recommendations focus on transparency/arms trade mechanisms, airspace governance and dual-use export controls. Together, these three interconnected areas will shape Europe's ability to understand, attribute and constrain the proliferation and misuse of drone technologies.

II. DRONE THREAT COMES TO EUROPE

Countering the spillover effects from Russia's war against Ukraine will require an aperture wider than the battlefield itself. Europe faces a layered drone threat from two directions. The eastern drone vector raises the problem of sovereign airspace violations as a result of either hostile border probing or a war collateral accident. Stranded Ukrainian drones have been found in Latvia, Finland and Estonia, most probably due to technical failure or a third party's electronic interference. Russia has regularly used navigation signals jamming in the Baltic and Black Sea regions, creating hazards for civilian aviation and maritime transport.³

Since February 2022, Russian drones have been confirmed in Croatia, Latvia, Lithuania, Moldova, Poland and Romania. In the largest incident, on 10 September 2025, over the course of seven hours, approximately 20 Russian drones flew deep into Polish territory before

¹ European Commission, 'Defence Readiness Roadmap, 2030', Brussels, Oct. 2025.

² European Commission, 'Action Plan on Drone and Counter Drone Security', Brussels, 11 Feb. 2026.

³ Osula, P., 'Estonia losing drones to Russian GPS interference', ERR, 30 Jan. 2025.

being intercepted by Polish and Dutch jets or crashing.⁴ In May 2026, Romania's most serious experience of Russian drone incursions resulted in civilian casualties.⁵ The Russian authorities tend to deny responsibility, either claiming that their drones do not have the range or blaming Ukrainian defence systems.⁶

These cross-border drone incidents are highly visible, attributable and escalatory. In this pattern of border violations, drones are not merely disruptive. Russia's drone incursions are part of its broader grey-zone campaign against Europe, alongside cyber operations, sabotage and coercive rhetoric.⁷ Russian drone ventures into European airspace are intelligence collection tools. Their purpose is to test defence readiness, including command and control, reaction times and force disposition, as well as to erode public confidence in the political resolve of the authorities.⁸

The Russian drone threat therefore follows a broader pattern of frequent airspace violations, sabotage of critical infrastructure and malicious cyber activities.⁹ NATO air-policing aircraft have intercepted Russian military aircraft hundreds of times each year since 2022.¹⁰ These sentry deployments extend to the maritime domain, given the concerns over Baltic and Arctic seabed sabotage.

Some observers find it difficult to identify appropriate responses due to the lack of clarity regarding the intent behind the drone incursions. However, uncertainty about intent plays into the logic of hybrid warfare—and makes attribution inherently political, based on a defender's general threat perceptions. A drone entering from Belarus, Russia or Ukraine is not simply a safety issue.¹¹

The drone threat does not come only from the east. Its southern vector involves dual-use drone technologies that enable illicit drug trafficking through criminal networks, as well as armed groups operating across North Africa and the Sahel.¹² In fragile environments shaped by armed proxy groups and weak international law enforcement, drones can become instruments of destabilization. The southern vector should not be underestimated.¹³ Cheap hobbyist drones are increasingly being used in smuggling, trafficking and other illicit activity along Europe's southern borders. States such as Bulgaria have recognized the importance of implementing stronger counter-drone measures to curb criminal drone activities.¹⁴

There has been a stark increase in the use of drones for lethal effect by violent non-state actors since 2022. The United Nations Security Council Counter-Terrorism Committee has registered the growing concern about the continued flow of misused commercially available drone technologies to illegal armed groups and criminals. Terrorist use of one-way-attack drones with operational autonomy to attack critical infrastructure has caused delays, panic and operational shutdowns across the Middle East and Central Africa.¹⁵

There is more serious concern regarding North Africa and the Sahel, which open-source data and field reporting indicate is one of the regions most affected by drone-related incidents and casualties.¹⁶ In addition to Turkish and Chinese platforms, commercial drones adapted for surveillance, strike and one-way improvised explosive delivery proliferate among armed groups and criminal actors due to increased knowledge-sharing, emulation and digital integration.¹⁷

⁴ Liang, X., 'NATO downs Russian drones over Poland', *Arms Control Today*, Oct. 2025.

⁵ Krupa, J., 'NATO says drone that crashed in Romania was "of Russian origin" despite Moscow's denials, as it happened', *The Guardian*, 29 May 2026.

⁶ Fix, L. and Dumbacher, E., 'Russia tests NATO with Poland drone breach', Council on Foreign Relations, 10 Sep. 2025.

⁷ Edwards, C. and Seidenstein, N., 'The scale of Russian sabotage operations against Europe's critical infrastructure', International Institute for Strategic Studies, 19 Aug. 2025.

⁸ Bremer, M. K. and Grieco, K. A., 'Hybrid air denial: The new gray zone battleground raging above Europe', *Defense News*, 2 Oct. 2025.

⁹ North Atlantic Treaty Organization, 'Statement of condemnation by the North Atlantic Council concerning Russian malicious cyber activities', 18 July 2025.

¹⁰ Ruitenberg, R., 'NATO intercepts of Russian aircraft stable in 2024 over prior year', *Defense News*, 13 Jan. 2025.

¹¹ European Parliament, Joint Motion for a Resolution on a united response to recent Russian violations of the EU member states' airspace and critical infrastructure, 7 Oct. 2025.

¹² Koné, H. and Koné, F. R., 'Sahel militants turn civilian drones into deadly weapons', Institute for Security Studies, 8 July 2025.

¹³ Independent Expert Group Supporting NATO's Comprehensive and Deep Reflection Process on the Southern Neighbourhood, Final Report, May 2024.

¹⁴ Sofia News Agency, 'Bulgaria to introduce criminal liability for unpermitted drone operations', Novinite, 10 Apr. 2025.

¹⁵ United Nations Security Council, Counter-Terrorism Committee Executive Directorate (CTED) and the Organization for Security and Co-operation in Europe (OSCE), *Physical Protection of Critical Infrastructure Against Terrorist Attacks: Trends Report Update* (CTED and OSCE: New York and Vienna, Nov. 2025).

¹⁶ Lyammouri, R. and Milnes, N., 'Drone warfare and cartel convergence in West Africa: Risks to American safety, security, and prosperity', Policy Center for the New South, 19 Sep. 2025.

¹⁷ NATO Strategic Direction, South Hub, *Proliferation of Drones and New Technologies in the Sahel*, Allied Joint Force Command Naples (JFCNP), Italy and Centro para El Bien Común, Madrid, Dec. 2025.

Table 1. Drone threat on the arms control radar

Drone technology development	Security implications	Arms control issue	Recommendation
New models	Explosion of drone purchases without accurate monitoring	Dormant arms trade regulations	Update arms transfers mechanisms
Cost asymmetry	Airspace ambiguity	Escalation risks	Improve underdeveloped airspace governance
Opaque supply chains	Sanctions evasion	Illicit drone proliferation	Close loopholes in the EU dual-use export control regime

The Russian footprint in Africa, channelled through the Africa Corps (formerly the Wagner Group), raises the possibility that today's drone threat from the south could degenerate from criminal activity to hybrid warfare thanks to the strong presence of Moscow-controlled irregular armed groups.¹⁸ Since Russia displaced western actors and reshaped the regional security environment, the EU has been guilty of a growing strategic blindness towards Sahel-originated threats from terrorism and violent extremism, organized crime and foreign information manipulation and interference.¹⁹

The last type of drone incursions is drones launched from within a state's territory to be flown near airports, military facilities, nuclear sites or logistics hubs, disrupting commercial activity and creating fear among the population. In the course of the autumn of 2025, unauthorized drones shut down airports in Copenhagen, Oslo and Munich, and led to air traffic closures around Brussels. Belgium also reported possible foreign-interference overflights near nuclear power plants and military sites such as the Kleine-Brogel air base.²⁰ Germany reported hostile drones over military facilities and Liquefied Natural Gas terminals, while Italy reported repeated overflights of the EU's nuclear research centre.²¹

Some observers label such drone interference hybrid air denial.²² These drone incidents are consequential not only because they violate airspace regulations, but

also because they demonstrate how low-cost drones can be used to disrupt traffic and commercial activities, imposing outsized costs on critical infrastructure and exposing gaps in local airspace governance.

However, while drones have been observed in multiple cases, very little information reaches the public about any investigation into who was operating the device or where it flew from. Few such investigations have found conclusive evidence of instances of foreign interference. The rapid increase in false alarms across Denmark, Finland, Germany, Latvia and Lithuania has led to a vocabulary change from drone incidents to 'aerial observations'.²³ An unclassified evaluation of aerial observations by the Danish Armed Forces notes that this issue has its roots in the insufficient training of local law enforcement units, their lack of capacity to detect, identify and intercept a suspicious drone, and slow information sharing with other agencies.²⁴ To counter public unease regarding the spike in aerial observations, the relevant authorities are increasingly expected to issue a public attribution, or at least an explanation.²⁵

Europe therefore faces a layered drone threat shaped by hybrid warfare from Russia, illicit drone use by criminal actors and accidental or ambiguous incursions that have important safety and reputational implications. Not every drone incident is the same and not every response should be military. A drone endangering air traffic at an airport can raise a local safety issue (in case of a fly-away drone) or a police security problem (in case of a terrorist attack or sabotage). A cross-border drone incursion is a violation of international law. An organized crime network using commercial drones raises an illicit trafficking or smuggling problem. Treating all these challenges

¹⁸ Arduino, A., 'Drones, disinformation and guns-for-hire are reshaping conflict in Africa: New book tracks the trends', *The Conversation*, 3 Aug. 2025; and TASS, 'Russian military-technical cooperation with Africa returns to level seen during Soviet era', 30 Jan. 2026.

¹⁹ Horák, L., 'Strategic blindness in the Sahel: Russian influence and EU security', *Obrana a Strategie*, vol. 26, no. 1 (2026), pp. 119–38.

²⁰ Rostampour, S. C., 'Drone incursions in Belgium spark probes, NATO-EU response', *Arms Control Today*, Dec. 2025.

²¹ Urbancik, J., 'Russian spy drones over Germany turn into an even greater threat', *EuroNews*, 10 Sep. 2025; and Reuters, 'Italy investigates drone flyovers of EU facility, spying suspected', 31 Mar. 2025.

²² Bremer and Grieco (note 8).

²³ Harmsen, P., 'Drone fever', *Weekendavisen*, 29 June 2026.

²⁴ Forsvaret, 'Resume af evaluering af Forsvarets indsats ifm. luftobservationer', 3 June 2026.

²⁵ Slonovska, S., 'West needs "escalation ladder" for Putin's shadow war', *CEPA*, 11 June 2026.

as one technical detection-and-interception task oversimplifies the issue. In all these cases, however, miscalculation could turn such low-cost attacks into expensive escalation. Importantly, a hostile airborne drone dramatically exposes the long-term failures of arms control and dual-use export control mechanisms.

III. SECURITY GOVERNANCE RAMIFICATIONS

The EU has progressively tightened its controls intended to restrict Russia's access to battlefield-relevant goods and technologies. This has included expanding export restrictions on dual-use and advanced technologies, stronger due diligence requirements and measures targeting entities in third countries involved in circumvention. Recent sanctions packages have also specifically targeted actors supporting Russia's drone production and supply chains.²⁶ These steps underscore the fact that Russian procurement networks are still able to exploit intermediaries, third country transshipment routes and widely traded commercial components. EU policymakers must now urgently seek ways to improve sanctions implementation and enforcement, as well as supply-chain visibility, without imposing disproportionate controls on legitimate dual-use trade.

Three broader security challenges stem from recent drone developments, all of which require the active engagement of the arms control expert community (see table 1). First, innovation in new lethal drone models has led to their rapid proliferation while arms control mechanisms remain focused on the drone wars of the 2010s. Second, cost asymmetry in favour of the attacker has contributed to a lowering of the barriers to drone operations while increasing ambiguity in airspace. Third, state and non-state actors can acquire dual-use drone technologies through opaque supply chains that enable illicit drone proliferation.

Drone innovations and lagging arms control reports

Russia's war against Ukraine has done more than intensify drone use. It has redefined what drone warfare looks like. For much of the past two decades, armed drones have been associated with the fight against international terrorism in the Middle East and Africa. They were large, expensive systems designed

to surveil from above and deliver missiles from afar. Ukraine—and now Iran—have changed the script from exquisite platforms to scalable strike systems. In other words, drone warfare is increasingly defined by drones as ammunition, rather than as delivery systems.²⁷ This dilemma of 'mid-tier' weapons, such as drones and man-portable defence systems, combines the monitoring challenges of traditional small arms and light weapons with the firepower of advanced conventional munitions.²⁸ The reshaped parameters of military technological competition require clearer drone reporting categories and better levels of state reporting to improve transparency in the global trade in drones.

The term 'drone' now encompasses an array of very different systems. In the earlier period, lethal drones were treated in essence as crewless aircraft armed with missiles. Few drone platforms were used for missions beyond intelligence, surveillance and reconnaissance. Europe's own force structure still reflects that legacy. It includes the US MQ-9 family, Israeli Heron and Hermes systems, and the troubled EU flagship Eurodrone project still in development.²⁹ In contrast, contemporary warfare has created conditions that prioritize a new generation of low-cost combat drones.³⁰ Lethal drones are now often the weapon itself. Loitering munitions and one-way attack drones do not merely strike their target, they crash into it.

Russia's full-scale invasion of Ukraine has produced the first modern drone war in which systems of different sizes, costs and functions have transformed the battlefield. The most important development concerns weaponized first-person-view (FPV) drones. These are small, single-use systems assembled from commercially available parts and fitted with explosives to carry out strike missions. Their battlefield utility lies in their scale, speed of adaptation and cost-per-effect. In early 2026, FPV drones had become one of the key components of Ukraine's defence strategy, accounting

²⁶ Council of the European Union, '21st package of sanctions: EU hits Russian energy, financial services and crypto hard', Press release, 23 July 2026.

²⁷ Kunertova, D., 'Drones have boots: Learning from Russia's war in Ukraine', *Contemporary Security Policy*, vol. 44, no. 4 (2023), pp. 576–91.

²⁸ Spindel, J. and Carter, K. L., 'Beyond small arms: Conceptualizing mid-tier weapons in conventional warfare', *International Studies Perspectives*, 24 July 2026.

²⁹ International Institute for Strategic Studies, 'Uninhabited Europe', Strategic Dossier 2026, *UAVs: ISR, Deterrence and War*, London, 26 Mar. 2026, pp. 23–37.

³⁰ Kunertova, D., *Embracing Drone Diversity: Five Challenges to Western Military Adaptation in Drone Warfare*, King's College London Freeman Air and Space Institute, Research Paper no. 29 (Apr. 2025).

for an estimated 60–80 per cent of Russian battlefield losses.³¹

In addition to the ongoing war in Ukraine, recent armed conflicts in the Middle East and tensions in the South China Sea have accelerated a new drone arms race in terms of low-cost, long-range, single-mission attack drones.³² Iran has pioneered the Shahed-136 model. Russia has industrialized production of its own Gerans. The United States has also embraced low-cost attritable attack drones.³³ These systems, which are expendable, destructive and relatively cheap, sit between tactical drones and conventional cruise missiles.

Since the beginning of 2026, Russia has launched around 140 Geran drones per day into Ukraine while producing over 3000 such drones per month.³⁴ Its estimated maximum range of 2500 kilometres means that the Geran-2 can reach much of Europe. China continues to broaden its portfolio of lethal drone systems, including new one-way attack models. The USA plans to acquire 300 000 low-cost drones by 2027 and has already combat-tested its Shahed-like LUCAS system in the Middle East.³⁵ Precise mass of cheap drones has become a defining feature of contemporary military competition.³⁶

Tracking drone transfers runs into a terminology problem. There are currently four broad categories of lethal drones. The first is the large armed aircraft platform, exemplified by systems such as the TB2 or Wing Loong. These are still important for surveillance and strike under favourable conditions. The second is the loitering munition, such as the Switchblade, Hero or Lancet, which can hover over an area to strike its target at the right moment. The third is the one-way attack drone, such as the Shahed/Geran and FPV drones, which flies a single, point-to-point strike

mission and detonates on impact. The fourth is the emerging category of collaborative combat aircraft, where autonomy, networking and human-machine teaming are the central features. These categories differ in function, cost, range, survivability and operational logic.

Whether a drone is treated as an aircraft, a missile or a munition has direct consequences for applicable export control rules and risk assessments. However, the arms trade and control mechanisms for lethal drones have not kept pace with drone realities. The result is incoherent reporting to the UN Register of Conventional Arms (UNROCA) and the Arms Trade Treaty (ATT), as well as irregularities and errors. UNROCA is a voluntary transparency and confidence-building mechanism intended to improve the visibility of conventional arms transfers and prevent destabilizing arms build-ups. The ATT establishes legally binding standards governing states parties' authorization of international conventional arms transfers, including measures against diversion. In UNROCA's annual reporting templates, drones tend to be scattered across three different categories: in Category IV as unmanned combat aerial vehicles, in Category V as rotary-wing unmanned combat aerial vehicles and in Category VII as remotely piloted vehicles with the characteristics of missiles capable of delivering a warhead or weapon to a range of at least 25 kilometres.³⁷

Current reporting guidelines do not oblige states to report attritable short-range one-way-attack drones that behave like mass munitions. Small modular quadcopters and FPV drones would appear to fall in the gap between Category V and Category VII.³⁸ Furthermore, due to their varying designs, drones are often reported in the wrong category. Drone platforms with kinetic payloads, for example, are sometimes listed in missile categories. In other cases, states misclassify imported and exported drones as manned combat aircraft or rely on national templates that are not comparable with UNROCA datasets. Just a brief exploration of annual reports indicates either that countries are not aware of this 'missile category option' or that their drones-as-ammunition go under the radar because their range is less than 25 km, as is the case

³¹ Watling, J. and Reynolds, N., *Tactical Developments During the Third Year of the Russo–Ukrainian War* (Royal United Services Institute: London, 2025), p. 10; and Ministry of Defence of Ukraine, "Army of Drones Bonus" program delivers results: Nearly 820,000 Russian targets hit in 2025, says Mykhailo Fedorov", 26 Jan. 2026.

³² Plichta, M. and Rossiter, A., 'A one-way attack drone revolution? Affordable mass precision in modern conflict', *Journal of Strategic Studies*, vol. 47, nos 6–7 (2024), pp. 1001–31.

³³ Lopez, C. T., 'War Department asks industry to make more than 300K drones, quickly, cheaply', *US Army*, 3 Dec. 2025.

³⁴ Anokhin, I., 'Monthly analysis of Russian Shahed 136 deployment against Ukraine', Institute for Science and International Security, 1 May 2026.

³⁵ Suciu, P., 'The US military is using Iran's own drones against it', *National Interest*, 4 Mar. 2026.

³⁶ Horowitz, M. C., 'Battles of precise mass', *Foreign Affairs*, 22 Oct. 2024.

³⁷ United Nations Register of Conventional Arms, 'Categories of major conventional arms', accessed 2 Mar. 2026.

³⁸ United Nations Secretariat, Group of Governmental Experts on the United Nations Register of Conventional Arms, 'The UN Register of Conventional Arms: Developments, trends, challenges and opportunities', 16 Feb. 2022.

with most loitering munitions such as Switchblade 300, L-Spike 1x or Kargu.

The MTCR adds a further layer by seeking to limit transfers of missile and unmanned aerial systems and related technologies capable of delivering weapons of mass destruction. Its controls are divided into Category I systems capable of carrying a 500-kg payload over 300 km and Category II, which covers drones with ranges of 300 km or more that fall below the Category I payload threshold, as well as related equipment, software and technology. However, many of the smaller, shorter-range, commercially derived lethal drones that have become prominent in contemporary conflicts remain outside or at the margins of these arrangements, complicating efforts to build a complete picture of their proliferation and transfer.

Furthermore, although states are requested to report their international arms transfers to the United Nations, major exporters and buyers of armed drones have failed to submit their reports for several years and UNROCA has no enforcement mechanism. The ATT, even though legally binding, suffers from a related weakness as major lethal drone exporters and importers have either not signed (Algeria, Azerbaijan, Eritrea, Ethiopia, India, Iran, Pakistan, Russia and Sudan) or not ratified (Israel, Türkiye, Ukraine, United Arab Emirates and the USA) it.³⁹ The treaty also allows reports to exclude commercially sensitive or national security information. In addition, reporting has deteriorated over time. The report submission rate under the ATT regime has declined from 87 per cent to 62 per cent since the treaty entered into force in 2014.⁴⁰

In sum, existing categories and divergent national reporting practices make it difficult to produce complete or comparable data on contemporary lethal drone transfers, particularly for smaller and shorter-range systems. UNROCA and ATT mechanisms need to align better with drone realities in order to promote oversight of the trade in lethal drones. Their lack of clarity about which drones are covered and where they should be reported is compounded by more systemic problems, such as the overall level and quality of states' engagement with these instruments.

Cost asymmetry and airspace ambiguity

The widening spectrum of lethal systems poses a new challenge for traditional air defences across Europe. This is especially true for the categories of 'packable' and 'truckable' drones, which can be moved easily and launched with only limited infrastructure. Combined with open-source designs, dual-use supply chains and the availability of components on global markets, commercial and consumer drone technologies present the challenge of cost asymmetry that leads to increasing ambiguity in airspace.

The EU has already begun to respond to these risks in its February 2026 Action Plan on Drone and Counter-Drone Security and the associated Drone Security Package, which contain measures on registration, identification, border surveillance and counter-drone response. These initiatives indicate that the challenge is increasingly recognized at the EU level. However, implementation remains dependent on national authorities and important differences persist in detection capacity, operational responsibility and the rules governing responses to non-cooperative drones.

The idea of a drone wall has practical value for defending against drones that violate sovereign airspace. This layered architecture combines acoustic communication, radio surveillance, cameras, radars, and jamming and kinetic interception capability to detect and counter low-flying objects along Europe's eastern border. Estonia in 2024 described a drone wall as a system of systems for persistent surveillance and denial in lower airspace.⁴¹

Countering domestic drone threats presents a different problem from drone defence on the frontline. Jamming, spoofing and high-energy interceptors present safety risks in crowded skies while hard-kill options create the problem of debris falling into populated areas. For these reasons, countering hybrid air denial operations around critical infrastructure cannot be treated as a military mission. Drone threats are a domestic security problem that requires adequately equipped local police forces and specialized units.

Deploying anti-drone systems at major international airports and nuclear power plants enhances a country's chances of responding to unauthorized drone activities. A common problem, however, is that local law enforcement has neither the training nor the

³⁹ Arms Trade Treaty, UN member states that have not yet joined the ATT, 23 Sep. 2025; and Arms Trade Treaty, ATT signatories that have not yet ratified, accepted or approved the treaty, 23 Sep. 2025.

⁴⁰ Arms Trade Treaty, Annual Reports, accessed 21 Sep. 2026.

⁴¹ ERR News, 'Estonia boosts €12 million drone wall to counter eastern border threats', 13 Nov. 2024.

equipment to react to aerial observations, let alone to neutralize suspicious drones.

Importantly, understanding drone interference as a hybrid tactic suggests that even the best air defences are unlikely to prevent Russia from launching drones into the sovereign territory of European countries. Such drone interference increases the probability of a miscalculation that could result in overreaction. European responses must therefore prioritize reduction of escalation risks through better airspace governance.

Addressing airborne drones is therefore not just a matter of sensors and interceptors, but also one of legal frameworks, organizational adjustments and the availability of technical equipment. A clear division of labour among the military, border police, regional and federal police, intelligence services, airport operators and critical infrastructure owners is essential to avoid confusion and slow reaction times.

In terms of legal authority, constitutional or statutory prohibitions prevent national armed forces from simply being deployed against domestic drone threats. Until February 2026, for example, the German Armed Forces could not shoot down drones inside Germany. The Aviation Security Act had to be amended to allow the armed forces to support police against drones, shifting authority to the Ministry of Defence.⁴² Similarly, in February 2025, Romania's parliament adopted legislation to allow the army to destroy, neutralize or take control of drones that breach Romanian airspace.⁴³

However, without a clear operational picture, speedy action can contribute to errors and escalation. Countering an active drone threat requires early warning sensors, real-time situational awareness, good information sharing and mobile counter-drone capabilities that can be rapidly deployed. An incident near Fort Hancock, Texas, provides a cautionary tale of a lack of inter-agency coordination that resulted in confusion between the Federal Aviation Administration and the Pentagon, leading to the shooting down of a US Customs and Border Protection drone, which had been mistaken for a cartel drone, using a high-risk counter-unmanned aircraft system—a high-energy laser weapon.⁴⁴

The EU's Single European Sky regulatory framework was not designed with an active airborne drone threat in mind.⁴⁵ The EU's drone rules were developed to integrate hobbyist and commercial drone manufacturers and operators into civilian airspace to support the drone economy. Based on a safety-first approach, this framework requires drone operators to follow rules depending on the weight and the specifications of the civil drone and the operation it is intended to conduct. Of the three categories of civil drone operations, 'open', 'specific' and 'certified', the majority of leisure drone activities and low-risk commercial activities are in the open category, which does not require a pilot licence or flight authorization, except in restricted areas. NATO adopted a similar risk-based approach, in addition to its altitude/weight approach, to classify drones as low, moderate or high risk and determine the certification process and training of drone operators.⁴⁶

Crucially, however, EU member states vary widely in how they define and enforce restricted areas for drones, especially near external borders and critical infrastructure zones. Exposed countries, such as Bulgaria, Estonia, Poland and Romania, may need to broaden no-drone zones and make such restrictions permanent. A more coherent approach to establishing and enforcing drone prohibited areas along the EU's external borders is overdue.

The EU therefore tends to focus on regulating the low-altitude economy rather than confronting repeated airport disruption, hostile overflights and drone border incidents.⁴⁷ The drone incursions of the past year show that the EU regulatory framework needs tightening to help to address drone threats and risk reduction by adjusting the rules for operations near borders and critical infrastructure.

⁴² Press and Information Office of the German Federal Government, 'Strengthening drone defence', 26 Feb. 2026.

⁴³ Ilie, L., 'Romanian lawmakers adopt law to shoot down drones breaching airspace', Reuters, 26 Feb. 2025.

⁴⁴ Tanyos, F., 'Pentagon shoots down Customs and Border Protection drone in Texas, federal officials say', CBS News, 27 Feb. 2026.

⁴⁵ Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems; and Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

⁴⁶ Haider, A., 'Introducing NATO's new UAS training methodology', NATO Joint Air Power Competence Centre, Nov. 2024.

⁴⁷ Sandor, F. et al., *Drone Futures: Road to 2040* (Adapt Institute: Bratislava, Oct. 2025).

Opaque supply chains and sanctions evasion

Four years of war have turned Ukraine into a drone superpower.⁴⁸ From near zero, it has built a domestic drone industry that has registered more than 400 unique drone types and produces millions of combat-capable drones per year.⁴⁹ Ukraine's defence industry reached an estimated annual production capacity of 8 million FPV drones in 2025.⁵⁰ Ukraine has managed to scale up improvised drone innovation to the production of mass precision. However, China's unmatched volume of dual-use drone manufacturing and the opaque supply chains through which actors acquire their drone components leave arms trade and dual-use export control mechanisms ill-prepared for the post-war proliferation of small lethal consumer drones.

Ukraine's drone innovation has moved ahead of its production capacities. China's exports of consumer drone technologies have become strategically indispensable to both Russia and Ukraine, creating an important supply chain dependence.⁵¹ China's drone exports to Ukraine in 2024 'amounted to almost \$1.1 billion and increased more than threefold', compared to the previous year.⁵² No other country has the industrial manufacturing capacity to meet the high demand for drones and drone parts. Before February 2022, Chinese consumer drone company Da-Jiang Innovations (DJI) had an estimated global market share of 94 per cent.⁵³ Its drones and drone parts are now sold through a wide range of channels, from retail purchases and e-commerce platforms (such as Amazon, Alibaba and Temu) to volunteer networks, resellers, cross-border smuggling and indirect third-country sales.

Since 2022, China has replaced the West as Russia's primary source of battlefield-relevant technology. Reports estimate that as much as 90 per cent of all sanctioned technology and more than three-quarters

of Russia's critical wartime imports now originate in China.⁵⁴ On paper, China tightened its dual-use export control regime in 2024, but Beijing continues to supply critical drone components to Russia, such as electric motors, carbon fibre, optical fibre, anti-jamming antennae and 3D printers.⁵⁵ Importantly, China's drone export ban to Ukraine since 2023, alongside increased Chinese drone exports to Russia, has eroded Kyiv's earlier drone advantage by increasing costs and slowing production.⁵⁶ While overall Chinese imports increased by almost 34 per cent year-on-year in 2025, the share of Chinese parts in Ukraine's drones subsequently fell to 'about 38 per cent'; however, it would be extremely difficult to completely exclude cheap Chinese components.⁵⁷

China not only dominates global drone supply chains, but also actively contributes to export practices that circumvent sanctions. Up to 80 per cent of the sanctioned western components that reached Russia in 2024 came through China.⁵⁸ Chinese companies regularly relabel dual-use agricultural and industrial systems or components, such as engines, fuel pumps, navigation systems, semiconductors and routers, as ordinary goods.⁵⁹ Other practices can conceal the end-user through rerouting. A Russian citizen arrested for illegal exports of US-sourced microelectronics to Russia shipped chips to Russia through third countries such as Hong Kong and Switzerland.⁶⁰ Transnational re-export networks span Hong Kong, Kazakhstan, Kyrgyzstan, Malaysia, Serbia, Thailand, Türkiye and the United Arab Emirates. Additional intermediaries in the supply chain can also be used to obscure the final destination. Russia's military intelligence service

⁴⁸ Horowitz, M. C., Dumbacher, E. and Kahn, L., 'How Ukraine's drone innovation reversed Russia's momentum', Council on Foreign Relations, 12 June 2026.

⁴⁹ GLOBSEC, 'GLOBSEC Forum 2026: Key takeaways', Prague, 21–23 May 2026.

⁵⁰ National Security and Defense Council of Ukraine, 'Results of Ukraine's defense industry in 2025: FPV drones', 23 Jan. 2026.

⁵¹ Golod, V. and Burtsev, D., 'China's drone war in Ukraine', *The Diplomat*, 24 Jan. 2026.

⁵² National Institute for Strategic Studies, 'Зовнішня торгівля України товарами: підсумки 2024 року [Ukraine's foreign trade in goods: Results for 2024]', 29 Jan. 2025.

⁵³ Singh, I., 'Drone analyst report reveals dramatic drop in DJI's commercial drone market share', *DroneDJ*, 14 Sep. 2021.

⁵⁴ US-China Economic and Security Review Commission, 'China-Russia fact sheet: A short primer on the relationship', 20 Aug. 2026.

⁵⁵ State Council of the People's Republic of China, 'China issues regulations on export control of dual-use items', 19 Oct. 2024.

⁵⁶ Savchii, A. et al., *Building the Arsenal: Securing the Components to Sustain Combat Power* (Snake Island Institute, 2025).

⁵⁷ National Institute for Strategic Studies, 'Зовнішня торгівля України товарами: підсумки 2025 року [Ukraine's foreign trade in goods: Results for 2025]', 18 Feb. 2026; and Varenikova, M., 'Ukraine reaches a milestone: Making "China-free" drones', *New York Times*, 11 Mar. 2026.

⁵⁸ Estonian Foreign Intelligence Service, 'International Security and Estonia 2025', 20 Dec. 2024; and Bjoertvedt, E., 'Western goods and companies in Chinese exports to Russia', B4Ukraine, Norwegian Helsinki Committee and CORISK, Apr. 2025.

⁵⁹ Priolon, G., 'Chinese drone maker emerges as covert supplier to Russia, Libya and Sahel juntas', *Intelligence Online*, 5 Dec. 2025.

⁶⁰ US Attorney's Office, Washington, DC, 'Russian citizen arrested for illegally exporting US-sourced microelectronics with military applications to Russia', Press release, 16 Sep. 2024.

abroad has developed such convoluted schemes aimed at evading sanctions.⁶¹

The innovation path taken by Iran and Russia shows that low-cost attack drones can be built from commercially available components traded free of export restrictions or supplied through chains that circumvent sanctions and dual-use control lists. For instance, drone cooperation between Russia and Iran has turned the Caspian Sea into a prime sanctions evasion route. Tehran has exported Shahed 131/136 and Mohajer-6 models to Russia that can strike Ukraine's critical infrastructure. Moscow, in turn, has delivered confiscated western anti-tank and anti-aircraft systems to Iran.⁶² This illicit proliferation of drone technologies poses a security threat to European countries through their use against Ukraine and by contributing to the export of affordable weapons to proxies in sub-Saharan Africa.⁶³

Limiting the import of Chinese consumer drone technologies is difficult when there are no affordable and reliable European alternatives. Despite cybersecurity concerns, the Estonian Defence Forces use Chinese-made DJI drones.⁶⁴ Similarly, the EU collaborates with DJI on geofencing guardrails to limit drone mobility and/or access in designated locations. This decision is based on price and availability, since western alternatives are not available in large quantities at present and cost three times as much.

Ukraine demonstrates that European countries need high-volume, short-range kinetic interceptors. Since 2024, it has deployed dedicated FPV drone interceptors such as Sting, which cost up to \$2500 each.⁶⁵ Europe's best chance of defending against the growing Russian drone threat is through stronger industrial partnerships that support domestic production capacities rather than continued dependence on foreign technology. The United Kingdom's Project Octopus is a

promising example of a joint development programme with Ukraine on innovation in drone interceptors.⁶⁶

IV. POLICY RECOMMENDATIONS

The regulatory mechanisms for arms trade, dual-use exports and airspace governance have not kept pace with drone-related technological developments. A lack of policy attention increases the risk of escalation and creates a permeable environment for the illicit proliferation of lethal drones. The following recommendations for the EU and European governments address the layered character of the drone threat in Europe.

Update dormant arms trade regulations

Europe has a drone problem that goes beyond the drone wall. The current drone threat slips under the radar of global arms trade instruments. Rapid drone innovation cycles and the spread of new lethal drone types have outpaced existing transparency and reporting arrangements, making it difficult to build a complete and comparable picture of international transfers. As a result, existing trade mechanisms and divergent interpretations of risk assessment rules often obscure rather than clarify the transfer of strike-enabled drones and drone technology exports.⁶⁷

EU member states, with support from the EU High Representative, should promote greater international dialogue on the classification, reporting and transfer of contemporary lethal drones through relevant UN and ATT processes. Despite the adoption of the EU common rules on the control of export of military technology and equipment in 2008, arms export authorizations remain largely a national competence.⁶⁸ While recognizing the limited prospects for major consensus-based reform, EU member states that are MTCR partners should, where feasible, use technical and policy discussions within the regime to clarify the treatment of evolving Unmanned Aerial Vehicle systems.

Any serious effort to improve oversight must involve major exporters and importers of lethal drones, not

⁶¹ Estonian Foreign Intelligence Service, 'International security and Estonia, 2026', 10 Feb. 2026.

⁶² Fricke, K., Hankins, T. and Jones, V., 'Two to tango: Russian-Iranian drone cooperation', *NATO Defense College Outlook Paper* no. 8 (9 July 2025).

⁶³ Grise, M. and Evans, A., 'The drivers of and outlook for Russian-Iranian cooperation', Rand Corporation, 4 Oct. 2023; and Pili, G. et al., 'Playing the long game: Russia in the Mediterranean', *NATO Defense College Outlook* 3/2025.

⁶⁴ Voltri, J., 'Chinese drones still dominate in Estonian Defense Forces training', *ERR News*, 19 Jan. 2026.

⁶⁵ Livingstone, K., 'These are Ukraine's \$1,000 interceptor drones the Pentagon wants to buy', *Military Times*, 11 Mar. 2026.

⁶⁶ UK Prime Minister's Office and Ministry of Defence, 'UK-Ukraine joint statement: Enhanced Security and Defence Industrial Collaboration Declaration', Press release, 17 Mar. 2026.

⁶⁷ Kunertova, D., 'The Iran conflict edges the world closer to a new drone arms race', *Bulletin of the Atomic Scientists*, 17 Mar. 2026.

⁶⁸ Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment.

just the states already most committed to transparency. The lack of accurate data on lethal drone transfers is a serious security issue. For this reason, the US-led 2016 initiative on the responsible export and use of armed drones now requires both revival and revision.⁶⁹ Thus far, efforts to initiate a multilateral dialogue at the General Assembly on lethal drones and their implications for international security and warfare have received only a limited response.⁷⁰

Low-cost, one-way attack drones, weaponized commercial quadcopters and strike-enabled dual-use systems blur the line between military and civilian technologies and weaken the link between the role assumed in the export category and actual battlefield use. For instance, the MTCR was designed to limit proliferation of systems capable of carrying a 500-kilogram payload at least 300 kilometres but this threshold logic captures only the largest drones. Most single-mission, long-range, low-cost systems such as the Shahed-136, LUCAS or Geran-2 fall awkwardly outside the stricter Category I as they meet only the range criterion. The regime's technical parameters are too rigid and encourage the development of drone strike capabilities just below the threshold of a 500-kg payload. At the same time, the Category II control list could accommodate this most dynamic end of today's lethal drones and their dual-use components, especially as countries have greater flexibility to evaluate transfer applications on a case-by-case basis compared to the strong presumption of denial for Category I items.

Importantly, the excessively tech-centric character of existing standards seems to have become counterproductive. US national export control is loosening to expedite drone sales and increase the competitiveness of US systems, framed as an 'America First Arms Transfer Strategy'.⁷¹ Both reinterpreting MTCR rules to treat drones as aircraft under Category II and expanding export licence exemptions on the export of small dual-use drones (or defining them as consumable commodities) weaken international

regulatory guidelines.⁷² Instead of using the MTCR as a reference framework, an alternative approach to controlling lethal drones could pay attention to where a system sits in the reconnaissance-strike framework.⁷³ Clearer terminology and coherent reporting practices should reflect operational function rather than airframe characteristics.

Improve underdeveloped airspace governance to reduce escalation risks

A small quadcopter near a civilian airport is not the same problem as a long-range drone violating sovereign airspace. Unauthorized or suspicious drone activity, either in the form of foreign drone interference or accidental fly-away drones, can quickly slide towards crisis through miscalculation. Reducing escalation risks therefore begins with transparent skies. The goal should be to make low-altitude airspace accessible to responsible operators and visible in the case of trespassers.⁷⁴ A real-time single picture of air traffic is an obvious risk-reduction tool that would help the authorities to distinguish routine activity and accidental breach from malicious use.

The February 2026 Action Plan and its Drone Security Package represent a move in the right direction for three reasons. Most importantly, they seek to strengthen the identification and accountability of drone operations. The package extends registration and identification requirements to all drones above 100 grams and includes direct remote identification and prevention of take-off unless an operator identification number has been entered. These are ways to reduce the number of unidentified objects in European airspace. Broader registration requirements and tighter accountability rules should leave both national and local authorities better placed to determine early on whether a drone pilot is compliant, reckless or potentially hostile.

Second, the concept of digital airspace allows better use of geofencing. This may include measures limiting

⁶⁹ Under-Secretary for Public Diplomacy and Public Affairs, 'Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Vehicles (UAVs)', US Department of State, 28 Oct. 2016.

⁷⁰ Permanent Mission of Portugal to the United Nations, 'Joint Statement on increasing multilateral exchanges of views regarding armed Uncrewed Aerial Vehicles', 22 Mar. 2024.

⁷¹ Executive Office of the President, Executive Order 14383 Establishing an America First Arms Transfer Strategy, 6 Feb. 2026; and Yousif, E. and Stohl, R., 'The "America First arms transfer strategy" reorders US arms transfer priorities', Stimson Center, 12 Feb. 2026.

⁷² Kuramitsu, S., 'US reinterprets MTCR rules to fast track drone sales', *Arms Control Today*, Oct. 2025; and US Department of Commerce, Bureau of Industry and Security, 'Streamlining export controls for drone exports', 21 Jan. 2026.

⁷³ Sanders, G. et al., 'Rising demands and proliferating supply: The future of the global UAS market', *Excerpt from the Proceedings of the Twentieth Annual Acquisition Research Symposium*, Naval Postgraduate School, Monterey, CA, 30 Apr. 2023, pp. 192–93.

⁷⁴ Bremer, M. K. and Grieco, K. A., 'Four things to know about hybrid air denial', *Lawfare*, 7 Dec. 2025.

a drone's connectivity, as well as future technical conditions and functionalities that will help prevent drones from entering prohibited or high-risk areas unintentionally. However, Europe still depends in part on foreign technology suppliers.⁷⁵ DJI's Fly Safe system has long provided voluntary GPS-based geofencing as a safety feature that prevents drones from flying too close to airports, prisons and power plants. Since January 2026, all DJI's class-labelled products have relied solely on official data published by national aviation authorities. Collaboration between DJI and the EU Aviation Safety Agency (EASA) could improve compliance and accuracy. However, that a sensitive part of Europe's regulatory airspace architecture still involves Chinese technology highlights an uncomfortable dependence. Furthermore, while technical safeguards can raise barriers to the hostile use of drones, they remain vulnerable to hacking and other methods of circumvention.⁷⁶

Third, the plan boosts protection of the EU's external borders. In addition to detection capabilities, it launches a counter-drone deployment initiative and a €250 million investment in land and maritime border surveillance. New national Rapid Counter-drone Emergency Response Teams, analogous to the EU Hybrid Rapid Response Teams, as well as EU-funded law enforcement networks are intended to provide cross-border coverage and mobile units for deployment at high-risk events.

Countering non-cooperative drones and malicious interference along external borders would benefit from a common EU legal and operational framework, since the rules for drone engagements are fragmented across countries. National investment in early detection and rapid reaction capabilities, such as the European Commission's Directorate General for Defence Industry and Space (DG DEFIS) co-funded Drone and Counter Drone European Resolve (DECODER), could prevent cheap interference from producing disproportionate effects in terms of economic and psychological costs. Another example of progress is participation in multinational operations such as Eastern Sentry, which could provide a framework for

authorizing use of military force.⁷⁷ NATO activity reinforces vigilance along the eastern flank by coordinating additional fighter aircraft, helicopters, transport aircraft, air-defence systems, surveillance assets and maritime platforms.

Close loopholes in the EU dual-use export control regime to combat illicit drone proliferation

While Europe invests in drone countermeasures, Russian drones continue to contain western components.⁷⁸ Loopholes in dual-use export controls linked to fragmented regulation across different national jurisdictions and poor post-sale monitoring enable countries under EU sanctions to obtain EU-produced components and use them to produce drones. EU member states should continue to close gaps that allow the drone threat to proliferate by tightening licensing and strengthening compliance monitoring. The Commission's DG Trade should regularly update and clarify the rules on dual-use export authorization within and outside the EU.

The EU only regulates dual-use exports at the EU level. Intra-EU dual-use transfer licensing still covers only a narrow category of items.⁷⁹ In addition, due diligence obligations are underdeveloped, there is limited guidance on risk assessment and compliance practices for exporters are uncertain. Public scrutiny of licensing decisions is weak, information-sharing on licence denials is limited and post-export monitoring is inconsistent.⁸⁰ Member states also continue to diverge in their interpretation of embargoes and sanctions, while enforcement capacity is uneven.⁸¹

The war in Ukraine has already revived discussion of these problems. The 2023 compilation of national control lists improved cross-country coordination. The September 2025 update of the EU dual-use control list,

⁷⁷ NATO Supreme Headquarters, Allied Powers Europe, 'Eastern Sentry', accessed 11 Mar. 2026.

⁷⁸ Yurchenko, A., 'Investigation: How Russian drones exploit European technologies to strike Ukraine, and beyond', *Kyiv Independent*, 18 Feb. 2026.

⁷⁹ Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items.

⁸⁰ Tricoli, J., 'EU export controls are failing to address the spread of spyware', Center for Democracy and Technology, 4 Dec. 2025.

⁸¹ Sabatino, E., 'Arms supplies to Ukraine: Does the European arms export control system need revision?', *EU Non-Proliferation and Disarmament Papers*, no. 89 (May 2024), p. 4.

⁷⁵ European Union Aviation Safety Agency, 'EASA and DJI collaborate to improve awareness of safe and legal drone operations', 22 Jan. 2026.

⁷⁶ Afowork, H. et al., 'Developing human rights guidelines for commercial drone manufacturers', McGill University, Max Bell School of Public Policy, 23 July 2026.

going beyond the Wassenaar Arrangement, showed that Brussels can circumvent Russia's veto.⁸²

Furthermore, the 2024 directive on shared definition of criminal offences and the application of penalties also addresses arms embargo circumvention.⁸³

European countries are becoming increasingly aware that countering drone proliferation requires systematic international coordination with different stakeholders from government and industry. In view of systematic sanctions evasion and the gaps in dual-use tech export control mechanisms, there is an urgent need for closer cooperation with law enforcement authorities, as well as stronger scrutiny of professional shell company creators and companies previously involved in goods transit to Russia.⁸⁴ Soft law tools can help too, such as a stronger code of conduct on drone production, sales and data services built around due diligence and responsible-by-design principles.⁸⁵

In future, AI integration is poised to increase the scope and scale of drone threats and their hybrid character. In particular, growing autonomy is likely to cloak perpetrators with greater plausible deniability, complicating attribution. It will be important to continue ethical and legal norm entrepreneurship and remain engaged with the UN Group of Governmental Experts on Lethal Autonomous Weapons Systems, as well as the 2023 Political Declaration on Responsible Military Use of AI and Autonomy.

V. CONCLUSIONS

European responses should not just be about how to counter an incoming airborne drone threat for the least amount of taxpayers' money. They should also seek to reduce ambiguity, contain proliferation and prevent cheap drone interference from becoming a pathway to escalation. European countries should therefore push in three directions.

First, they should work towards a drone regulation classification based more explicitly on their use in

combat, rather than on technology alone. This could mean, for instance, focusing the discussion among MTCR partners on whether the drone behaves like a missile, ammunition or a platform. However, the diverging US interpretation of MTCR rules and Russia's participation in the MTCR—as in the case of the Wassenaar Arrangement—substantially reduce the short-term prospects for agreement on major revisions, given the regime's consensus-based decision making.

The EU, through its long-standing outreach activities in support of ATT implementation, is uniquely positioned to create impetus for an international discussion on lethal drones in the ATT Secretariat and the United Nations General Assembly. Rapid drone developments require policy action to align terminology and reporting practices with existing instruments. A one-way attack drone that functions as a slow-flying strike munition should not be hidden in categories designed for a different era. New standards setting should result in better awareness of current mechanisms, shared practices on reporting and a stronger common understanding of lethal drones.

Second, local detection and identification that widen early-warning windows, together with coherent rules of engagement for drone emergencies informed by EASA and the European Commission, would reduce the risk of accidents and inadvertent escalation. European capitals doubling down on research and development into novel anti-drone measures could prove a crucial investment. However, DG DEFIS funding mechanisms should ensure that the drone wall is built without technologies that originate from outside NATO or EU member states, while keeping defences affordable. Importantly, escalation prevention should include specialized training for engineers, pilots, border units and local law enforcement to enhance their responsiveness.

Third, European countries should press for broader participation in and better compliance with dual-use technology export control authorizations. This can begin at the EU level with the European Commission and the Council of the European Union revisiting and clarifying the criteria in the EU legislation regulating dual-use technologies inside the EU market. Additional post-sale controls would further strengthen measures against sanctions circumvention. The EU's dual-use export control regime would also benefit from the introduction of dynamic procedures for determining which dual-use technologies require enhanced end-use and end-user monitoring.

⁸² The 1996 Wassenaar Arrangement sets standards for the export of dual-use drone technologies and enables export information sharing, albeit on a voluntary basis. All EU member states except Cyprus are members of the Wassenaar Arrangement and the EU aligns its trade rules with the group.

⁸³ Directive (EU) 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) 2018/1673.

⁸⁴ Estonian Foreign Intelligence Service (note 61), p. 49.

⁸⁵ Bromley, M. and Maletta, G., *The Militarization of Technology: Preventing Diversion and Misuse Through Export Controls* (SIPRI: Stockholm, Nov. 2025).

ABBREVIATIONS

ATT	Arms Trade Treaty
DG DEFIS	Directorate General for Defence Industry and Space
DJI	Da-Jiang Innovations
EASA	EU Aviation Safety Agency
EU	European Union
FPV	First-person-view
MTCR	Missile Technology Control Regime
NATO	North Atlantic Treaty Organization
UNROCA	UN Register of Conventional Arms

LIST OF RECENT NON-PROLIFERATION AND DISARMAMENT PAPERS

EU Policy Engagement on Advanced Conventional Weapons and Sanctions Compliance in the South Caucasus

Non-Proliferation and Disarmament Paper no. 101
Giorgi Goguadze
August 2026

Cyber (Dis)armament in Practice: The EU's Role in Governing Software Vulnerabilities in a Fragmented International Order

Non-Proliferation and Disarmament Paper no. 100
Eugenio Benincasa
May 2026

The Australia Group at 40: Making the AG Fit for an Era of Geopolitical Competition

Non-Proliferation and Disarmament Paper no. 99
Kolja Brockmann
June 2025

Cloud Labs and Other New Actors in the Biotechnology Ecosystem: Export Control Challenges and Good Practices in Outreach

Non-Proliferation and Disarmament Paper no. 98
Kolja Brockmann, Lauriane Héau and Giovanna Maletta
May 2025

Lessons from the EU on Confidence-building Measures Around Artificial Intelligence in the Military Domain

Non-Proliferation and Disarmament Paper no. 97
Sofia Romansky
May 2025

The EU as a Key Player in Multilateral Forums on Space Security: Perspectives for the OEWG 2025–28

Non-Proliferation and Disarmament Paper no. 96
Mathieu Bataille
April 2025

Non-proliferation, Nuclear Technology and Peaceful Uses: Examining the Role and Impact of Export Controls

Non-Proliferation and Disarmament Paper no. 95
Giovanna Maletta, Dr Mark Bromley and Kolja Brockmann
April 2025

The EU Research Security Initiative: Implications for the Application of Export Controls in Academia and Research Institutes

Non-Proliferation and Disarmament Paper no. 94
Lauriane Héau
March 2025

Subregional Arms Control and Conflict Prevention in the Western Balkans

Non-Proliferation and Disarmament Paper no. 93
Katarina Djokic
January 2025

Artificial Intelligence, Non-proliferation and Disarmament: A Compendium on the State of the Art

Non-Proliferation and Disarmament Paper no. 92
Dr Thomas Reinhold, Dr Elisabeth Hoffberger-Pippan, Dr Alexander Blanchard, Marc-Michael Blum, Dr Filippa Lentzos and Alice Saltini
January 2025

The Potentially Revolutionary Impact of Emerging and Disruptive Technologies and Strategic Conventional Weapons on the Nuclear Deterrence Debate

Non-Proliferation and Disarmament Paper no. 91
Tom Sauer
December 2024

The Nexus of Non-traditional Security and Nuclear Risk: Implications for EU Foreign Policy in the Indo-Pacific

Non-Proliferation and Disarmament Paper no. 90
Elin Bergner, Sarah Laderman and Marcy R. Fowler
November 2024

Arms Supplies to Ukraine: Does the European Arms Export Control System Need Revision?

Non-Proliferation and Disarmament Paper no. 89
Ester Sabatino
May 2024

What Happened To Demand? Getting Small Arms Control Back on Track

Non-Proliferation and Disarmament Paper no. 88
Callum Watson and Aline Shaban
March 2024



This document has been produced with the financial assistance of the EU. The contents are the sole responsibility of the EU Non-Proliferation and Disarmament Consortium and can under no circumstances be regarded as reflecting the position of the EU.

A EUROPEAN NETWORK

In July 2010 the Council of the European Union decided to support the creation of a network bringing together foreign policy institutions and research centres from across the EU to encourage political and security-related dialogue and the long-term discussion of measures to combat the proliferation of weapons of mass destruction (WMD) and their delivery systems. The Council of the European Union entrusted the technical implementation of this Decision to the EU Non-Proliferation Consortium. In 2018, in line with the recommendations formulated by the European Parliament, the names and the mandate of the network and the Consortium have been adjusted to include the word 'disarmament'.

STRUCTURE

The EU Non-Proliferation and Disarmament Consortium is managed jointly by six institutes: La Fondation pour la recherche stratégique (FRS), the Peace Research Institute Frankfurt (HSFK/ PRIF), the International Affairs Institute in Rome (IAI), the International Institute for Strategic Studies (IISS–Europe), the Stockholm International Peace Research Institute (SIPRI) and the Vienna Center for Disarmament and Non-Proliferation (VCDNP). The Consortium, originally comprised of four institutes, began its work in January 2011 and forms the core of a wider network of European non-proliferation and disarmament think tanks and research centres which are closely associated with the activities of the Consortium.

MISSION

The main aim of the network of independent non-proliferation and disarmament think tanks is to encourage discussion of measures to combat the proliferation of weapons of mass destruction and their delivery systems within civil society, particularly among experts, researchers and academics in the EU and third countries. The scope of activities shall also cover issues related to conventional weapons, including small arms and light weapons (SALW).

www.nonproliferation.eu

EU Non-Proliferation and Disarmament Consortium

Promoting the European network of independent non-proliferation and disarmament think tanks



**FOUNDATION FOR
STRATEGIC RESEARCH**

www.frstrategie.org



**PEACE RESEARCH INSTITUTE
FRANKFURT**

www.hsfk.de



INTERNATIONAL AFFAIRS INSTITUTE

www.iai.it/en



**INTERNATIONAL INSTITUTE
FOR STRATEGIC STUDIES**

www.iiss.org/en/iiss-europe



**STOCKHOLM INTERNATIONAL
PEACE RESEARCH INSTITUTE**

www.sipri.org



Vienna Center for Disarmament
and Non-Proliferation

**VIENNA CENTER FOR
DISARMAMENT AND NON-
PROLIFERATION**

www.vcdnp.org