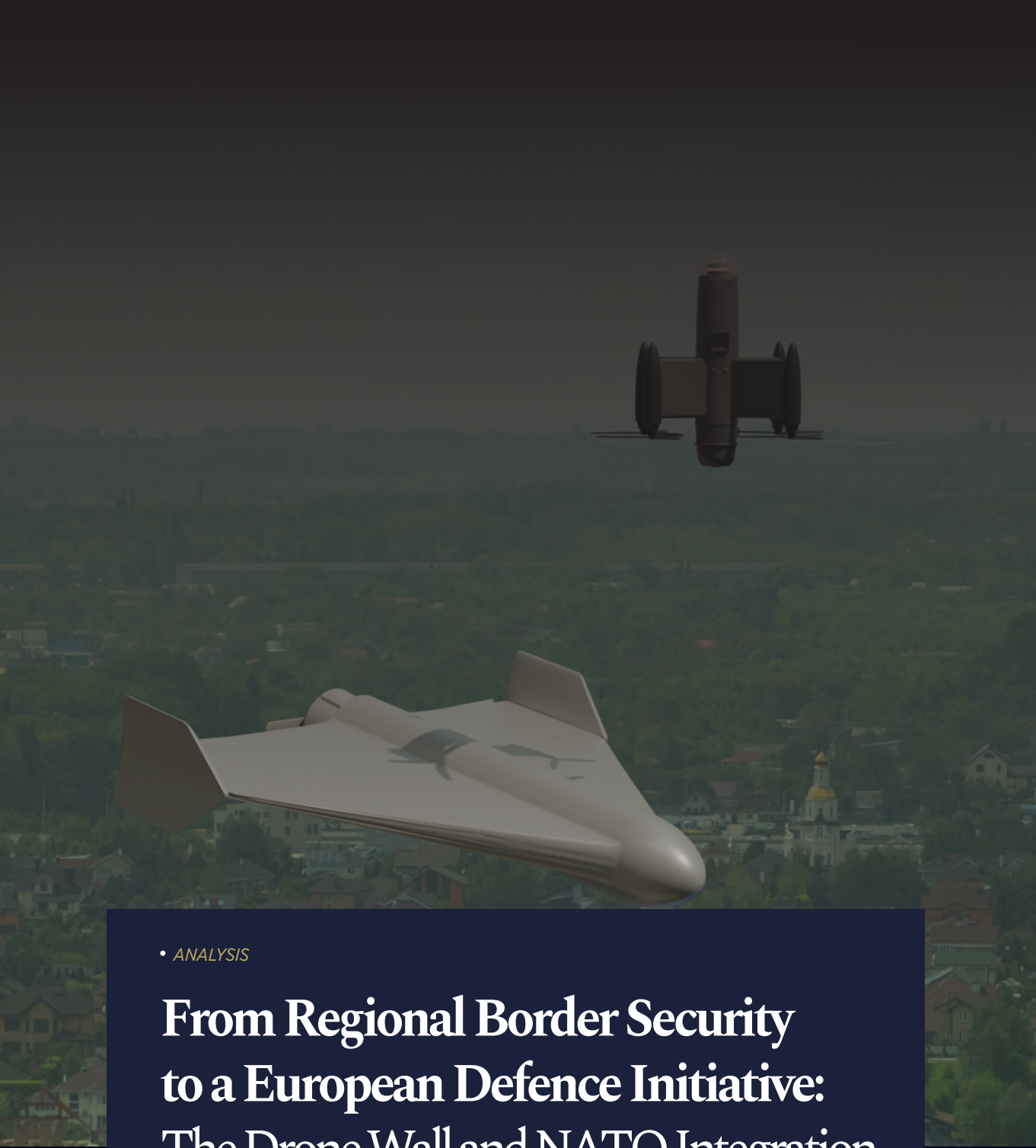


• *ANALYSIS*

From Regional Border Security to a European Defence Initiative: The Drone Wall and NATO Integration

Sibel Düz

www.setav.org

20.yıl | SETA

JULY 2026 NO 107

FROM REGIONAL BORDER SECURITY TO A EUROPEAN DEFENCE INITIATIVE: The Drone Wall and NATO Integration

SİBEL DÜZ

SETA

SETA Yayınları
ISBN: 978-625-5703-67-5

Editorial Team: Ebrar Üzümcü, Sudib Sontoran, Gizem Akbaş
Layout: Said Demirtaş

SETA | SİYASET, EKONOMİ VE TOPLUM ARAŞTIRMALARI VAKFI
Nenehatun Cd. No: 66 GOP Çankaya 06700 Ankara TÜRKİYE
Tel: +90 312 551 21 00 | Faks: +90 312 551 21 90
www.setav.org | info@setav.org | @setavakfi

SETA | İstanbul
Defterdar Mh. Savaklar Cd. Ayvansaray Kavşağı No: 41-43
Eyüpsultan İstanbul TÜRKİYE
Tel: +90 212 395 11 00 | Faks: +90 212 395 11 11

SETA | Washington D.C.
1025 Connecticut Avenue, N.W., Suite 1106
Washington D.C., 20036 USA
Tel: 202-223-9885 | Faks: 202-223-6099
www.setadc.org | info@setadc.org | @setadc

SETA | Berlin
Kronenstraße 1, 10117 Berlin GERMANY
berlin@setav.org

SETA | Brussels
Avenue des Arts 27, 1000 Brussels BELGIUM
Tel: +3226520486

CONTENTS

SUMMARY | 7

INTRODUCTION | 8

THE DRONE THREAT TO NATO'S EASTERN FLANK | 10

- Drone Incursions and Airspace Violations | 10
- Hybrid Threats and Persistent Surveillance | 11
- Protection of Critical Infrastructure | 11
- The Problem of Low-Cost Attrition | 12

LIMITATIONS OF EXISTING AIR DEFENCE ARCHITECTURES | 12

FROM A REGIONAL BORDER SECURITY INITIATIVE TO A EUROPEAN DEFENCE INITIATIVE | 13

THE EUROPEAN DRONE WALL AND THE STRATEGIC AXIS | 16

THE ARCHITECTURE OF THE DRONE WALL AND NATO INTEGRATION | 18

THE CONTRIBUTION OF THE DRONE WALL TO DETERRENCE, DEFENCE, AND RESILIENCE | 22

RISKS | 23

CONCLUSION | 24

This analysis examines the evolution of political approaches to the Drone Wall concept, its place within NATO's air and missile defence agenda, and the key parameters shaping its transformation into an Alliance-integrated counter-unmanned aerial systems (C-UAS) defence architecture.

SUMMARY

The Drone Wall should be assessed not merely as a technical initiative designed to strengthen border security against the growing unmanned aerial vehicle threat on Europe's eastern flank, but as a multi-layered counter-drone defence approach that needs to be integrated into NATO's deterrence and defence architecture. The Russia–Ukraine war has clearly demonstrated the capacity of low-cost drones and decoys to attrite air defence systems, deplete munition stocks, place critical infrastructure under pressure, and generate political-military risks within NATO airspace. Therefore, the strategic value of the Drone Wall depends not on the destruction of individual targets, but on its ability to integrate early warning, persistent surveillance, reliable identification, a shared air picture, proportionate engagement, and the protection of critical assets within a single architecture. Within this framework, the European Union can play a complementary role in financing, industrial scaling, regulation, and critical infrastructure security. However, the definition of operational requirements, the establishment of interoperability standards, and the testing of the concept in collective defence scenarios should remain NATO-centred. Otherwise, the Drone Wall may remain a politically visible but fragmented border surveillance project. If properly designed, however, it could evolve into a feasible defence layer that strengthens deterrence, force protection, and operational resilience against low-cost, high-volume, and hybrid unmanned threats on the eastern flank.

INTRODUCTION

With the Russia–Ukraine war, unmanned systems have begun to assume a key role on the battlefield by performing central military functions rather than serving merely as secondary tactical tools. Indeed, Ukraine and Russia have employed unmanned aerial vehicles (UAVs)[1] not only for situational awareness and kinetic strikes, but also to impose costs on the adversary, deplete air defence stocks, and conduct perception and effects-oriented operations.

The war has not remained confined to the territories of the two countries, it has also affected NATO airspace. On 9–10 September 2025, following the violation of Polish and Romanian airspace by Russian drones, NATO launched Operation Eastern Sentry, and the Alliance eliminated the threat through F-16 and F-35 aircraft.[2] However, this episode also demonstrated that relying on high-end airpower, advanced defence systems, and expensive interceptor munitions against relatively cheap and expendable drones does not constitute a sustainable operational model for continuous defence.

1 Within the scope of this study, the terms "drone" and "UAV" (unmanned aerial vehicle) are used interchangeably and synonymously, without drawing a technical distinction between them.

2 "Russian Drone Incursions: Blurring the Line between Provocations and Probing", SETA, 17 September 2025, Accessed 3 July 2026, https://www.setav.org/en/russian-drone-incursions-blurring-the-line-between-provocations-and-probing; Sibel Düz, "Russian drones in NATO airspace: Probing leads Europe to 'Drone Wall'", Daily Sabah, 9 October 2025, Accessed 3 July 2026, https://www.dailysabah.com/opinion/op-ed/russian-drones-in-nato-airspace-probing-leads-europe-to-drone-wall ; "NATO launches "Eastern Sentry" to bolster posture along eastern flank", NATO, 12 September 2025, Accessed 3 July 2026, https://www.nato.int/en/news-and-events/articles/news/2025/09/12/nato-launches-eastern-sentry-to-bolster-posture-along-eastern-flank

In fact, in 2023, Baltic countries such as Lithuania, Latvia, and Poland advanced the "Drone Wall" project in order to enhance border surveillance in response to migration flows from Belarus, which they believed were being instrumentalised by Russia and its regional ally Belarus to generate social and political instability in the region. However, applications submitted by the Estonian and Lithuanian governments for EU funding were rejected by the Commission.[3] The 2025 airspace violations, however, brought the significance of the project back to the fore. In order to close capability gaps, European countries have promoted several projects under the Defence Readiness Roadmap 2030, including Eastern Flank Watch, the European Drone Defence Initiative (EDDI), the European Air Shield, and the European Space Shield.[4] Through EDDI, it has been proposed that Europe's border defence capacity be developed comprehensively through multi-domain surveillance systems, UAV and counter-UAV capabilities, electronic warfare assets, precision-strike systems, and rapid operational coordination. In addition to the European Drone Defence Initiative, the European Commission's Drone and Counter-Drone Security Action Plan identifies preparedness, detection, coordinated response, industrial scaling, and defence readiness as core priorities.

> From NATO's perspective, the drone threat extends beyond the issues of airspace violations or isolated target engagements. Rather, it constitutes a multidimensional security challenge encompassing hybrid coercion, the protection of critical infrastructure, persistent surveillance, and low-cost attrition dynamics simultaneously.

On the basis of these initiatives, the "Drone Wall" should be analysed not as a fixed physical barrier, but as a network-centric counter-UAV defence architecture composed of sensors, data fusion systems, command-and-control systems, and neutralisation assets.

Moreover, a technically reliable Drone Wall would require persistent detection, credible identification, real-time tracking, rapid engagement options, and battle damage assessment along national borders. It would also require secure data exchange, common standards, shared air situational awareness, and procedures for civil-military cooperation. These requirements place the Drone Wall directly within NATO's broader air and missile defence agenda. The key issue in this respect is whether the European Drone Wall can evolve from a highly visible border-security initiative into a NATO-integrated counter-UAV defence architecture that strengthens deterrence and defence on NATO's eastern flank.

3 Justinas Lingevicius, Bruno Oliveira Martins, Giacomo Bruni , "From the Ground to the Stars: The Vertical Politics of the EU Drone Wall and Airspace Defence", Journal of Comman Market Studies, 26 February 2026, Accessed 3 July 2026, https://onlinelibrary.wiley.com/doi/10.1111/jcms.70092

4 "Readiness Roadmap 2030", Avrupa Komisyonu, 16 October 2025, Accessed 3 July 2026, https://defence-industry-space.ec.europa.eu/eu-defence-industry/readiness-roadmap-2030_en ; "Commission publishes the Action Plan on Drone and Counter-Drone Security", Avrupa Komisyonu, 11 February 2026, Accessed 3 July 2026, https://defence-industry-space.ec.europa.eu/commission-publishes-action-plan-drone-and-counter-drone-security-2026-02-11_en

This analysis will examine the shift in political approaches to the concept, the concept's relevance within NATO's air and missile defence agenda, and the parameters of its transformation into a NATO-integrated counter-UAV defence architecture.

THE DRONE THREAT TO NATO'S EASTERN FLANK

For NATO, the drone threat is not merely a matter of airspace violations or isolated target engagements. Rather, it constitutes a multi-layered security challenge that simultaneously encompasses hybrid pressure, critical infrastructure security, the need for persistent surveillance, and the dynamics of low-cost attrition.

DRONE INCURSIONS AND AIRSPACE VIOLATIONS

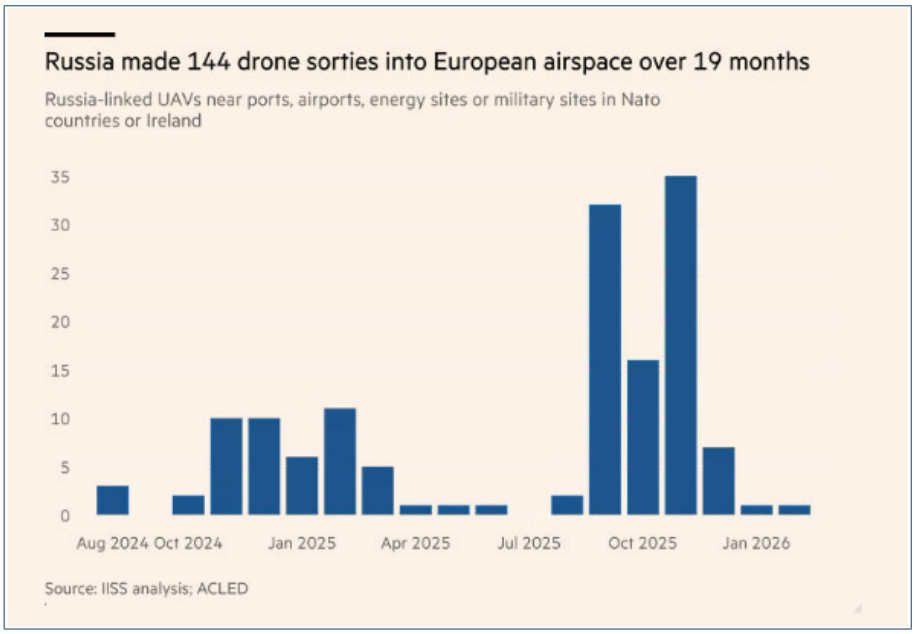
The Russia–Ukraine war has intensified military activity in proximity to NATO territory, including Russian attacks against targets near the Polish and Romanian borders. The war has also generated risks related to navigation errors, electronic interference, debris, and deliberate or unintended airspace violations.

In this context, one of the most significant incidents occurred on the night of 9–10 September 2025, when multiple Russian drones violated Polish and Romanian airspace. NATO activated its air defence posture and subsequently launched Operation Eastern Sentry.[5] NATO characterised the incident in Poland as part of a broader pattern of Russian behaviour and noted that other Allies had also experienced airspace violations. Poland also requested consultations under Article 4 of the North Atlantic Treaty.

Another incident took place on the night of 7 May 2026, when two Ukrainian one-way attack drones missed their intended Russian targets and struck four empty fuel tanks in a depot near Rēzekne in eastern Latvia. The episode culminated in the resignation of Latvian Defence Minister Andris Sprūds on 11 May, following intense political pressure after he stated that civilian security could not be guaranteed. On 20 May, following a suspected drone crossing from Belarus into Lithuania, President Gitanas Nausėda, Prime Minister Inga Ruginienė, and Defence Minister Robertas Kaunas took shelter in bunkers. This was recorded as the first instance since the beginning of the war in which the leaders of a NATO capital had entered shelters.[6]

5 "NATO launches "Eastern Sentry" to bolster posture along eastern flank"

6 "The Baltic Drone Spillover and the Drone Wall", Defence Ukraine, 27 May 2026, Accessed 3 July 2026, https://www.defenceukraine.com/en/insights/baltic-drone-spillover-nato-drone-wall/



Source 1 "Russian drone campaign mapped Nato air defence gaps, study finds", Financial Times, 2 July 2026, Accessed 3 July 2026, https://www.ft.com/content/49ed0040-7f5d-402d-b42d-1d8eab27114c

HYBRID THREATS AND PERSISTENT SURVEILLANCE

Drones can also be employed beyond conventional military purposes. They are widely accessible, relatively inexpensive, difficult to attribute, and capable of generating political effects without necessarily causing physical destruction. States and non-state actors may use them to collect imagery intelligence, monitor military movements, interfere with civil aviation, and conduct similar activities.

For this reason, a Europe-wide counter-drone architecture should not be built solely around target destruction. It also requires an information network capable of distinguishing routine civilian activity from potentially hostile behaviour.

PROTECTION OF CRITICAL INFRASTRUCTURE

Many facilities classified as critical infrastructure are located in urban areas, densely populated zones, or near civil aviation routes. Kinetic interception may create risks due to debris, missed engagements, or the uncontrolled fall of the target. Electronic jamming may disrupt communications, interfere with navigation, or affect emergency services. Automated engagement systems may also lack sufficient authority or identification confidence to act without human approval, thereby creating challenges for counter-drone defence. A balance must therefore be struck between aviation safety, public security, and proportionality.

Critical infrastructure defence also creates a prioritisation challenge. The role of each asset in military mobility, command and control, energy supply, civil

continuity, and national resilience must be determined. It is necessary to identify which assets are strategically critical, which are more exposed to threats, and which have limited redundancy.

THE PROBLEM OF LOW-COST ATTRITION

Throughout the war, Russia has made extensive use of one-way attack drones and lower-cost decoys in order to destroy targets, complicate identification, deplete defensive stocks, and expose air defence positions. Ukraine, for its part, has employed commercial and custom-built drones for surveillance, attack, deception, and interception missions. The use of one-way attack drones and decoys can generate significant combat mass while also imposing considerable pressure on air defence.[7]

Accordingly, the problem is not merely one of increasing the number of high-end systems. The defensive mix must correspond to the cost, scale, and characteristics of the target. A counter-drone architecture is therefore expected to analyse effectively the cost relationship between unit cost, production volume, launch density, and existing munition stocks. It should not simply seek the lowest cost per engagement, but rather select the appropriate balance among probability of kill, target value, munition depth, and operational risk.

LIMITATIONS OF EXISTING AIR DEFENCE ARCHITECTURES

The need for a Drone Wall should be assessed through the design limitations of traditional air defence, the difficulties of detecting small UAVs, cost-imposition dynamics, and saturation risks.

Traditional air defence architectures were developed primarily to counter manned aircraft, helicopters, cruise missiles, and ballistic missiles. Many European countries have reduced their short-range air defence stocks and directed air defence investments toward higher-altitude aircraft and missile threats. Small drones, by contrast, exploit the lower layer of the airspace, where sensor coverage, engagement authority, and suitable effectors may be limited. For this reason, the strategic role of the Drone Wall should be to strengthen the low-altitude and short-range layer.

In addition, it is well established that characteristics such as small size, low altitude, low speed, and limited radar cross-section make small UAVs difficult to detect by traditional air surveillance systems.[8] Detection, however, does not

7 "Fortifying NATO's eastern flank ", IISS, 24 February 2026, Accessed 3 July 2026, https://www.iiss.org/publications/the-military-balance/2026/the-military-balance-2026/fortifying-natos-eastern-flank/

8 "A Comprehensive Approach to Countering Unmanned Aircraft Systems ", Joint Air Power Competence Centre, 2021, Accessed 3 Temmmuz 2026, https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf

necessarily amount to identification. A radar track may indicate the presence of an object, but it may not reveal its type, payload, operator, or intent. For this reason, no single sensor should be expected to provide reliable coverage in every environment. This is the principal reason why the Drone Wall concept emphasises layered and distributed sensing. Geographic conditions further complicate this coverage problem. For example, a sensor configuration suitable for Poland's open terrain may not deliver the same performance in Finnish forests, Baltic coastal areas, or urban environments. Detection gaps are not merely a technical problem, they also constitute a vulnerability with strategic consequences. The defence architecture should therefore be designed not as a static structure, but as an adaptive system that continuously evolves in response to the threat environment.

> The necessity of a Drone Wall should be assessed in light of the design limitations of conventional air defence systems, the challenges associated with detecting small unmanned aerial systems (UAS), cost-imposition dynamics, and the risks posed by saturation attacks.

Air defence is also not limited to physical interception. It is also a competition over resources, industrial capacity, readiness, and opportunity costs. The Drone Wall can improve the cost relationship in three ways. Better detection and classification can reduce unnecessary interventions, while a layered effector model can enable countermeasures to be matched to the threat. Finally, shared surveillance can reduce duplication among national systems and allow resources to be concentrated in priority sectors.

The war in Ukraine has also demonstrated that saturation attacks can produce operational effects even when interception rates are high, since even a small proportion of successful penetrations can damage energy infrastructure, logistics hubs, air bases, or urban targets. Saturation attacks are often understood as a numerical problem in which the attacker launches more weapons or munitions than the defender has interceptors. In reality, however, they can affect every stage of the defensive chain. Sensors may struggle to maintain tracks in a dense and cluttered environment, communications may be disrupted, data fusion systems may generate more alerts than operators can assess, decision-makers may not have sufficient time to authorise engagements, and effectors may run out of munitions, power, or suitable firing positions. For this reason, a geographically distributed Drone Wall covering a wide area is required.

FROM A REGIONAL BORDER SECURITY INITIATIVE TO A EUROPEAN DEFENCE INITIATIVE

The Drone Wall concept was first advanced in 2023 by Lithuania, Latvia, and Poland as a regional border security initiative. It was later proposed in May 2024

by the interior ministers of Estonia, Latvia, Lithuania, Poland, Finland, and Norway as a coordinated system extending from Norway to Poland.[9]

The initial concept reflected the security concerns of states bordering Russia and Belarus. These countries had been confronted with migration, smuggling, electronic interference, border incidents, and broader Russian pressure. The proposed "wall" aimed to strengthen surveillance through UAVs, fixed sensors, and counter-drone capabilities. The original Drone Wall concept therefore corresponded to a technology-enabled border monitoring and surveillance network rather than an integrated air defence system. In this form, the concept shared common ground with Estonia, Lithuania, and Latvia's Baltic Defence Line[10] and Poland's East Shield[11] initiatives, which sought to reinforce border surveillance, mobility control, and defence preparedness.

By 2025, the Drone Wall had evolved from a regional border security concept into a broader European defence initiative. The main drivers of this shift were the intensification of drone activity in Ukraine, Russian hybrid activities, and drone threats emerging around military and civilian facilities in Europe. The violation of Polish airspace in September 2025 intensified the political debate by demonstrating that unmanned threats could directly activate NATO air defence mechanisms. In response, the European Commission was compelled to incorporate the concept into a broader defence readiness framework. The Defence Readiness Roadmap 2030 identified four strategic flagship projects: the European Drone Defence Initiative, the Eastern Flank Watch Initiative, the European Air Shield, and the European Space Shield.[12] This framework expanded both the geographic and functional scope of the original Drone Wall concept.

The European Drone Defence Initiative characterises the Drone Wall as a layered and interoperable system designed to detect, track, and neutralise hostile drones by drawing on Ukraine's battlefield experience. The Eastern Flank Watch Initiative, meanwhile, treats counter-drone capabilities within a broader framework by linking them to air defence, electronic warfare, ground surveillance, maritime situational awareness, and critical infrastructure protection.[13]

The Drone and Counter-Drone Security Action Plan, published in February 2026, further broadened the policy framework by addressing preparedness, multi-sensor detection, information sharing, critical infrastructure, external

9 "Baltics, Poland, Finland, Norway agree on 'drone wall' to protect borders ", LRT, 24 May 2024, Accessed 3 July 2026, https://www.lrt.lt/en/news-in-english/19/2281492/baltics-poland-finland-norway-agree-on-drone-wall-to-protect-borders

10 "Baltic Defence Line", ECDI, Accessed 3 July 2026, https://www.kaitseinvesteeringud.ee/en/baltic-defence-line/

11 "The Eastern Shield': How Poland wants to defend its borders from invasion ", Euronews, 7 September 2025, Accessed 3 July 2026, https://www.euronews.com/2025/09/07/the-eastern-shield-how-poland-wants-to-defend-its-borders-from-invasion

12 "Readiness Roadmap 2030"

13 "Eastern Flank Watch and European Drone Wall", Avrupa Palamentosu Think Tank, 21 October 2025, Accessed 3 July 2026, https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/777962/EPRS_ATA(2025)777962_EN.pdf

borders, civil-military coordination, industrial scaling, exercises, and regulatory reforms. It also explicitly recognised that Europe's drone challenge spans civil security, hybrid threats, and military defence.[14]

This transformation moves the Drone Wall beyond being merely an element of the EU's border security and counter-drone capability development agenda. It also raises the question of how the concept should be linked to NATO's deterrence and defence architecture.

The EU can make an important contribution to the Drone Wall in the areas of capability development, resilience, industrial scaling, and civil-military coordination. However, this contribution cannot substitute for NATO's central role in military command and collective defence. The Drone Wall should therefore be positioned not as a separate operational chain, but as an element that complements NATO's deterrence and defence architecture.

> The strategic value of the Drone Wall derives not merely from its capacity to detect and neutralize unmanned aerial systems, but from its ability to integrate early warning, persistent surveillance, proportionate counter-drone defence, critical infrastructure protection, and the resilience of NATO's eastern flank within a unified defence architecture.

In this context, the central issue is how national and EU-supported counter-drone capabilities will feed data into NATO's shared air picture, how they will support Allied decision-making processes, and under which command relationships they will be employed in a crisis or conflict. NATO's Integrated Air and Missile Defence (IAMD) Policy provides the principal doctrinal framework in this regard.[15] IAMD does not view the threat as limited to traditional aircraft and missiles. It covers a broad spectrum of threats, ranging from small, low-altitude, and low-speed drones to cruise missiles, ballistic missiles, and hypersonic threats. The policy also defines IAMD as a continuous mission that must be conducted without interruption in peacetime, crisis, and conflict, while placing emphasis on rapid detection, decision-making, and engagement processes. Counter-drone defence should also be treated as part of this integrated architecture. However, not every drone-related incident should require NATO's direct operational control. In many incidents occurring around airports, borders, public spaces, and critical infrastructure, national civil and military authorities should continue to bear primary responsibility.

The relationship between the Drone Wall and NATO IAMD should be established through the NATO Integrated Air and Missile Defence System (NATINAMDS). NATINAMDS constitutes the main implementation mechanism that brings together Allies' air surveillance, command-and-control, active defence, and passive defence capabilities. The 2025 policy defines this architecture

14 "Commission publishes the Action Plan on Drone and Counter-Drone Security"

15 "NATO Integrated Air and Missile Defence Policy ", NATO, 13 February 2025, Accessed 3 July 2025, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-integrated-air-and-missile-defence-policy

through four functional areas: air surveillance; battle management, command, control, communications, and intelligence; active air and missile defence; and passive air and missile defence.[16] The Drone Wall can be directly associated with these functional areas.

Accordingly, the strategic value of the Drone Wall depends on its ability to achieve integration across three levels. First, it must establish effective coordination between national military and civilian authorities. Second, the EU's capability development instruments must be aligned with NATO's operational requirements. Third, tactical-level counter-drone defence must be connected to a broader strategic framework aimed at deterring Russia's military and hybrid activities.

THE EUROPEAN DRONE WALL AND THE STRATEGIC AXIS

The diversity of threats directed at NATO's geographic area of responsibility is increasing day by day in parallel with technological transformation. The Alliance now faces a broad threat spectrum ranging from combat aircraft and ballistic missiles to loitering munitions, commercial quadcopters, AI-enabled systems, and autonomous platforms. NATO therefore requires a distributed, persistent, and integrated defence approach, particularly against unmanned threats.

The "Drone Wall" is a geographically distributed network of surveillance, command-and-control, and counter-drone capabilities. Through this network, the objective is to enhance the ability of NATO and national authorities to respond more effectively to unmanned threats by enabling early warning, countering low-altitude threats, and protecting selected assets.

The strategic logic of the concept rests on four propositions:

i. unmanned systems constitute a persistent threat to NATO airspace, military forces, and critical infrastructure,

ii. existing air defence forces should not respond to every low-cost target with high-end interceptor munitions and combat aircraft,

iii. national systems cannot effectively manage cross-border drone activity without shared information and coordinated procedures,

iv. the eastern flank requires a defence architecture that can operate in peacetime, crisis, and conflict without treating every unidentified drone as an act of war.

The strategic value of the Drone Wall derives not merely from its capacity to detect and neutralise unmanned aerial vehicles, but from its ability to integrate

16 NATO Integrated Air and Missile Defence", ", NATO, 13 February 2025, Accessed 3 July 2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/nato-integrated-air-and-missile-defence

early warning, persistent surveillance, proportionate counter-drone defence, critical infrastructure protection, and the resilience of the eastern flank within a single architecture.

The first strategic objective of the Drone Wall is to improve early-warning capability. Small drones can significantly compress decision-making timelines because they can fly at low altitude, exploit terrain or urban clutter, and be launched from points close to their targets. Early warning should therefore not be understood solely as the moment at which an object is first detected. The time required to confirm a track, classify it, assess its behaviour, transmit the information to the relevant authorities, and allocate an appropriate response element is also part of the early-warning process.

> The European Drone Wall should not be regarded as an autonomous barrier. Instead, it should be understood as a complementary layer within the broader policy architecture encompassing the NATO Integrated Air and Missile Defence System (NATINAMDS), the defence of the eastern flank, civil preparedness, infrastructure resilience, and measures designed to counter hybrid threats.

This capability should also support cross-border warning. A drone detected in one country may shortly thereafter move toward the airspace of another. For this reason, it is not sufficient to retain incident data at the national level alone, since incident data fused at the strategic level can reveal patterns that individual events may not show. Early warning thus acquires a broader function that encompasses both real-time tactical detection and long-term intelligence analysis.

The second objective is to establish persistent situational awareness of the low-altitude air environment. Persistent surveillance does not merely mean that sensors operate without interruption. This capability must also remain usable in adverse weather conditions, under electronic interference, and in a cyber-contested environment. Persistent surveillance also contributes to deterrence. An adversarial actor that expects to be detected may be forced to accept higher risk, employ more sophisticated platforms, or avoid certain targets. The aim here is not to eliminate all hostile surveillance activity entirely, but to make it less reliable and more costly.

At the same time, the surveillance architecture must also manage the risk of excessive data generation. In the absence of effective filtering, data fusion, and prioritisation mechanisms, additional data may complicate operators' decision-making processes rather than facilitate them. Surveillance therefore generates strategic value only to the extent that it improves the quality of decision-making.

The third objective is to provide proportionate and sustainable counter-drone defence. No single effector can neutralise every type of drone under all conditions. A layered approach is therefore required. Electronic countermeasures, for example, may be effective against platforms dependent on external links, but they produce limited results against drones using autonomous navigation. Artil-

lery systems and interceptor drones may provide cost-effective defence, but they can face constraints in terms of range, safety, and weather conditions. Missiles may offer a higher probability of kill, but they cannot be used as the default response tool against every low-cost target. The purpose of layered defence is to allocate the most appropriate and sustainable response according to the nature of the threat.

The fourth objective is to protect critical military and civilian assets. Air bases, ports, command facilities, ammunition depots, fuel installations, energy infrastructure, border crossings, railways, and key communications nodes may be among the priority areas in this regard. However, the precise selection of assets to be protected will depend on national risk assessments and NATO's operational plans. The protection model must take into account not only military effectiveness, but also civilian safety. Engagement options around airports and urban infrastructure require stricter legal and technical controls than those that may be applied around isolated military facilities.

The fifth objective is to strengthen resilience across the eastern flank. Drone defence can contribute to this objective by protecting critical functions, reducing uncertainty, and preserving the freedom of action of military and civilian authorities. From this perspective, the ultimate strategic contribution of the Drone Wall should be to provide decision-makers with time and to preserve operational freedom of action during a crisis or conflict.

The European Drone Wall should therefore not be assessed as an independent barrier. The concept should be treated as a complementary layer within NATO's Integrated Air and Missile Defence, eastern flank defence, civil preparedness, infrastructure resilience, and the broader policy architecture developed to counter hybrid threats.

THE ARCHITECTURE OF THE DRONE WALL AND NATO INTEGRATION

Differences in terrain, population density, climate, airspace organisation, and threat spectrum prevent the European Drone Wall from being designed as a system in which identical sensors and interceptors are deployed along a continuous line. A technically reliable architecture must therefore bring together wide-area surveillance, local protection, mobile capabilities, national command systems, and regional information exchange. The design should allow different national components to contribute to a common defence function without requiring participating states to procure the same equipment.

This approach can also be observed in NATO's current experimental work. Allied Command Transformation's (ACT) Layered Counter-Uncrewed Aircraft

Systems Initiative-Experimental (LCI-X) treats counter-drone defence as a challenge that requires the integration of sensors, command-and-control systems, electronic warfare tools, and effectors. Indeed, during the Crucible 1-26 event held in Romania in April 2026, NATO tested radars, acoustic and radio-frequency detectors, electronic warfare tools, and kinetic and non-kinetic effectors as part of an integrated counter-drone defence entity.[17]

Interoperability should therefore not be regarded as a secondary technical requirement, but as the central strategic variable of the Drone Wall. NATO defines interoperability as the ability of Allied forces, units, and systems to operate together coherently, effectively, and efficiently.[18] This definition goes beyond equipment compatibility and encompasses common doctrine, procedures, terminology, training, infrastructure, and trust-building. A functional counter-drone defence architecture must ensure technical, procedural, and human interoperability, at least at a minimum level.

> The success of the Drone Wall should be measured not only by the number of drones detected or neutralized, but also by governments' capacity to manage such incidents without generating public panic, operational paralysis, or disproportionate political responses.

Historically, NATO has operated with different armies and force structures, as well as various national platforms and doctrines, and has transformed this diversity into military coherence through standards, common doctrine, command arrangements, exercises, and information sharing. The Drone Wall should be built on a similar rationale. Different national sensors, command-and-control structures, counter-drone capabilities, and civil security elements can generate a common defensive effect only through a robust interoperability architecture.

The Drone Wall must therefore address three core dimensions of interoperability simultaneously. Technical interoperability refers to the ability of sensors, command-and-control tools, communication networks, databases, and effectors to exchange and use information. Procedural interoperability enables institutions and Allies to interpret the same data in broadly similar ways, allocate responsibilities consistently, and act in concert. Human interoperability creates the professional competence, mutual trust, and institutional familiarity that allow multinational procedures to function under crisis pressure.

The first test of technical interoperability is equipment and architectural diversity. Allies on the eastern flank operate different radars, air defence assets, communication systems, electronic warfare platforms, and national air surveillance

17 "Layered Counter-UAS Initiative (LCI-X) is Building NATO's Approach to a Fast-Moving Threat", NATO, 18 May 2026, Accessed 3 July 2026, https://www.act.nato.int/article/lci-x-builds-approach-fast-moving-threat/ ; "From Experimentation to Capability: LCI-X Crucible 1-26 in Romania", NATO, 24 April 2026, Accessed 3 July 2026, https://www.act.nato.int/article/lcix-1-26/

18 "What Is Interoperability — And Why It Matters to NATO", NATO, 15 May 2025, Accessed 3 July 2026, https://www.act.nato.int/article/what-is-interoperability/

networks. This diversity creates both advantages and challenges for the Drone Wall. The aggregation of different sensors and effectors may provide wider coverage, but non-standardised data formats, divergent track-quality criteria, and incompatible command-and-control interfaces can complicate the formation of a shared picture.

In this context, the United Kingdom's SAPIENT (Sensing for Asset Protection with Integrated Electronic Networked Technology) autonomous sensor architecture offers a notable example. In NATO technical interoperability activities, SAPIENT has been assessed as a potential basis for information exchange. However, SAPIENT should not yet be regarded as an established and binding Alliance-wide standard. Although the United Kingdom has adopted this architecture at the national level, NATO has not yet tested it comprehensively, and the architecture has not replaced existing NATO tactical data standards.[19]

The second technical challenge is data volume. Radars, electro-optical sensors, radio-frequency detectors, acoustic systems, and other detection tools operating in low-altitude airspace can generate very large amounts of data. Transmitting all raw data to national or NATO command centres would impose a significant burden on bandwidth, processing capacity, and operator attention. The Drone Wall architecture should therefore be based on a tiered processing approach. Raw data should be processed as close to the source as possible, while only meaningful tracks, confirmed threats, and information requiring decision-making should be transmitted to higher command layers.

The third challenge is latency. In counter-drone defence, detection, classification, decision-making, and engagement are often measured in seconds. Every technical interface, data conversion, and command transfer can add delay to the decision cycle. The effectiveness of the Drone Wall should therefore be measured not by how much data its sensors collect, but by whether the right data reaches the right decision authority at the right time.

The fourth challenge is track quality. Small drones may have a low radar cross-section, disappear among terrain features or urban structures, and be confused with birds, commercial drones, or other low-altitude movements. Technical interoperability must therefore support not only data sharing, but also track correlation, track confirmation, and classification reliability.

The fifth challenge is effector integration. Counter-drone defence may include electronic countermeasures, interceptor drones, artillery systems, directed-energy solutions, and, in certain circumstances, missile systems. Each of these tools has different ranges, costs, and engagement timelines. The Drone Wall should therefore be designed not merely as a network that detects threats, but as

19 "Guidance SAPIENT autonomous sensor system", GOV UK, 20 December 2021, Accessed 3 July 2026, https://www.gov.uk/guidance/sapient-autonomous-sensor-system

an architecture that matches the appropriate response option to the nature of the threat, the surrounding environment, and the rules of engagement.

Procedural interoperability concerns how Allies classify incidents, allocate responsibility, transmit warnings, hand over tracks, authorise responses, and assess outcomes. Technical systems may generate common data, but interoperability remains limited if there are no common procedures for interpreting that data. If one country labels an object as "hostile" while another interprets it as "unidentified but potentially threatening," the shared air picture may complicate decision-making rather than provide clarity.

> While the Drone Wall has the potential to make significant contributions to the defence of NATO's eastern flank, this architecture also entails important risks and limitations. These challenges can be grouped into four principal categories: technological dependence, escalating costs, governance challenges, and the emergence of a false sense of security.

NATO therefore needs to develop a common and graduated classification language for counter-drone defence. In such a language, identity, threat assessment, and attribution should be kept distinct. Identity concerns what the object is, threat assessment concerns what it may do or how dangerous it is, and attribution concerns who launched, directed, or controlled it. Conflating these three elements can create risks of false alarm, unnecessary escalation, or delayed response. Clear and common classification procedures would increase the consistency of Allied decision-making, particularly in cross-border drone incidents.

Human interoperability concerns the ability of personnel from different countries and institutions to understand one another, trust shared information, and apply common procedures under pressure. Counter-drone defence does not involve only air defence operators. It can bring together different actors around the same incident, ranging from political decision-makers and intelligence agencies to electronic warfare specialists and military command elements, each approaching the drone threat with distinct institutional priorities and risk perceptions.

Human interoperability therefore requires these different perspectives to be aligned before a crisis occurs. Through common training and exercises, it should be determined who will lead in which situation, which institution will require what type of information, how risk will be communicated, and according to which thresholds response decisions will be taken. However advanced the technical architecture may be, the decision cycle can slow down if personnel do not understand one another's authorities, procedures, and limitations.

Multinational staffing, that is, the assignment of personnel from participating states to regional centres, joint exercises, and counter-drone scenarios, can facilitate better familiarity with national authorities, technical systems, and oper-

ational procedures. The success of the Drone Wall will therefore depend not only on the quality of sensors or effectors, but also on the ability of the people using these capabilities to develop a shared operational culture.

THE CONTRIBUTION OF THE DRONE WALL TO DETERRENCE, DEFENCE, AND RESILIENCE

The European Drone Wall is an attractive initiative insofar as it seeks to eliminate low-altitude surveillance gaps, prevent cross-border drone incursions and critical infrastructure vulnerabilities, address the cost imbalance between low-cost drones and high-end interceptors, and enhance Allies' counter-drone capabilities. However, integrating these capabilities within a single multinational architecture entails significant operational, technical, financial, and institutional requirements.

For this reason, the initiative should be assessed not as a deployed defence system, but as an emerging capability concept. Since 2026, NATO and the EU have developed policy frameworks, experimentation programmes, funding mechanisms, and industrial initiatives related to counter-drone defence. NATO Allied Command Transformation's Layered Counter-Uncrewed Aircraft Systems Initiative has begun testing how sensors, command systems, electronic warfare tools, and effectors can operate as an integrated capability. The European Commission's Drone and Counter-Drone Security Action Plan has proposed measures covering detection, coordinated response, industrial production, testing, critical infrastructure protection, and civil-military cooperation. Taken together, these developments indicate growing political momentum and technical activity. Nevertheless, the strategic utility of a multinational Drone Wall for NATO should be assessed through its contribution to deterrence, defence, and resilience.

The Drone Wall's primary contribution to deterrence lies in reducing the likelihood that an adversary can achieve its intended objectives through UAV operations. In this sense, the concept rests primarily on the logic of deterrence by denial. Beyond its direct capacity for neutralisation, the Drone Wall may also generate indirect costs. An adversary may be forced to employ more platforms, develop lower-observable systems, rely on greater autonomy, alter launch points, or invest in countermeasures.

Although such an architecture is necessary for security and resilience, it should also be kept in mind that it cannot, by itself, constitute a strategic response to Russia's hybrid activities. It should further be noted that opportunity costs may arise if resources allocated to defensive measures are diverted from support to Ukraine or from other capabilities that could impose more direct costs on Russia.[20]

20 Daniel Hegedüs, "The Drone Wall It cannot remain Europe's answer to Russian hybrid warfare. ", GMF, 29 September 2025, Accessed 3 July 2026, https://www.gmfus.org/news/drone-wall

The Drone Wall should therefore be assessed as only one component of deterrence. Effective deterrence usually requires a combination of denial, punishment, resilience, strategic signalling, and escalation management.

From a defence perspective, the most tangible contribution of the Drone Wall is that it strengthens the lower layer of NATO Integrated Air and Missile Defence. European forces have well-known capability gaps in short-range and very short-range air defence. A distributed counter-drone defence network can enhance early warning, classification, and engagement capabilities against low-cost threats that do not require the use of high-end interceptors, while also helping to preserve more advanced air defence assets. Counter-drone components should not be considered separately from NATO's broader IAMD architecture, since the military value of the Drone Wall depends on its ability to operate as a complementary lower layer within that architecture. At this point, the institutional division of labour is also critical. NATO should define operational requirements and integrate the Drone Wall into the collective defence architecture. The EU, meanwhile, should play a complementary role in procurement, production, testing, regulation, innovation, industrial scaling, and civil-military preparedness.[21]

From a resilience perspective, malicious drone activity often aims less at direct destruction than at intimidation, disruption, and the erosion of public confidence. Public preparedness, crisis communication, and institutional coordination are therefore as important as technical response. The success of the Drone Wall should be measured not only by how many drones are detected or neutralised, but also by the capacity of governments to manage such incidents without generating panic, operational paralysis, or political overreaction.[22]

RISKS

The Drone Wall could make important contributions to NATO's eastern flank. However, this architecture also contains serious risks and limitations of its own. These risks can be examined under four main headings: technological dependency, cost escalation, governance challenges, and the emergence of a false sense of security.

The first risk is technological dependency, stemming from the Drone Wall's heavy reliance on digital networks, AI-enabled analytical tools, software and information infrastructures, and complex supply chains. While these elements can

21 Can Kasapoğlu, Peter Raugh, "How NATO Can Build Europe's Drone Wall", Hudson Institute, 17 November 2025, Accessed 3 July 2026, https://www.hudson.org/missile-defense/how-nato-can-build-europes-drone-wall-can-kasapoglu-peter-rough

22 Tim Chattell, "A 'Drone Wall' is needed for Europe to defend against a new threat ", Chatham House, 1 October 2025, Accessed 3 July 2026, https://www.chathamhouse.org/2025/10/drone-wall-needed-europe-defend-against-new-threat

enhance the performance of the architecture, they may also create new areas of vulnerability.

The second risk is cost escalation. Although the Drone Wall is often presented as a more sustainable defence solution against low-cost drones, the establishment and operation of this architecture will require significant expenditure. How these costs are shared within the Alliance and the EU will also constitute a political issue.

The third risk concerns governance challenges. The Drone Wall will be a complex architecture that intersects the areas of responsibility of NATO, the EU, national defence and interior ministries, border security agencies, civil aviation authorities, intelligence services, and similar institutions. In an architecture involving such a large number of actors, clarifying institutional responsibilities is as important as technical integration. Even differences in rules of engagement can create significant vulnerabilities in such architectures.

The fourth risk is the emergence of a false sense of security. The Drone Wall should not be presented as a barrier that provides absolute protection. Rather, it should be described as a distributed early-warning network, a regional situational-awareness architecture, a tool for protecting priority infrastructure, a lower-layer contribution to NATO IAMD, a mechanism linking national counter-drone capabilities, and an adaptive defence model. Otherwise, governments may neglect areas such as passive defence, dispersal, facility security, repair capacity, redundancy, and civil preparedness. Public opinion, meanwhile, may interpret every successful incursion as evidence that the entire architecture has failed. The performance of the Drone Wall should therefore be assessed on the basis of measurable outputs rather than political rhetoric.

CONCLUSION

The value of the Drone Wall for NATO lies not in establishing an independent and parallel defence arrangement, but in its functional integration into the existing deterrence and defence architecture. Implementation should therefore rest on a clear institutional division of labour. NATO should define military-operational requirements, embed counter-drone capabilities within Integrated Air and Missile Defence, establish interoperability standards, and test the architecture in collective defence scenarios. The European Union, in turn, should accelerate capability development and reduce fragmentation through its regulatory, financial, industrial, research, border-security, and critical-infrastructure instruments. Eastern Flank Allies should operationalise this framework through regional coordination, shared surveillance, harmonised procedures, and the protection of priority assets.

The success of this approach depends on defining counter-drone defence within NATO IAMD planning as a lower and distributed layer against persistent, low-altitude, and high-volume threats. Not every small drone incident needs to be elevated to NATO command channels. However, national and regional capabilities must be able to feed data into the shared air picture, use harmonised classifications in threat assessment, and rely on pre-defined arrangements for track handover and engagement authority during a crisis. It is therefore critical for NATO to develop an alliance-wide Counter-Drone Integration Strategy, define common technical and procedural standards, establish independent testing and validation mechanisms, and incorporate lessons learned from Ukraine into a continuous adaptation cycle.

Ultimately, if the Drone Wall is treated merely as a sensor, effector, or border-surveillance project, it will provide only a limited and fragmented contribution. Its real strategic value will emerge to the extent that it can connect NATO's operational requirements, the EU's capability-development instruments, regional needs on the eastern flank, and common standards generated through multinational exercises. The priority should therefore not be to create new institutional duplications, but to establish a permanent counter-drone knowledge, testing, and adaptation function through existing NATO structures, Centres of Excellence networks, ACT activities, technical exercises, and innovation environments. Such an approach could transform the Drone Wall from a politically visible initiative into a feasible architectural layer that strengthens deterrence, defence, and resilience on NATO's eastern flank.

SİBEL DÜZ

She obtained her degree in International Relations from the Middle East Technical University (Ortadoğu Teknik Üniversitesi) and commenced her career as a research assistant at the SETA Foundation in 2014. Presently, she holds the position of project coordinator for the Terrorism Analysis Platform (TAP), a comprehensive database and web portal initiated in 2019, which continues to actively operate. Since 2021, she has been engaged as a researcher at SETA. Notably, she has authored esteemed reports published by SETA, including "The Ascension of Türkiye as a Drone Power: History, Strategy, and Geopolitical Implications","Unpacking the Debate on Turkish Drones" and " Remote Control: Aerial Elimination of the PKK's Terrorist Leaders and Operatives". Her research pursuits predominantly revolve around military technology and strategy, counterterrorism and insurgency, as well as unmanned systems.

From Regional Border Security to a European Defence Initiative: The Drone Wall and NATO Integration

Sibel Düz

The Drone Wall should be assessed not merely as a technical initiative designed to strengthen border security against the growing unmanned aerial vehicle threat on Europe's eastern flank, but as a multi-layered counter-drone defence approach that needs to be integrated into NATO's deterrence and defence architecture. The Russia–Ukraine war has clearly demonstrated the capacity of low-cost drones and decoys to attrite air defence systems, deplete munition stocks, place critical infrastructure under pressure, and generate political-military risks within NATO airspace. Therefore, the strategic value of the Drone Wall depends not on the destruction of individual targets, but on its ability to integrate early warning, persistent surveillance, reliable identification, a shared air picture, proportionate engagement, and the protection of critical assets within a single architecture. Within this framework, the European Union can play a complementary role in financing, industrial scaling, regulation, and critical infrastructure security. However, the definition of operational requirements, the establishment of interoperability standards, and the testing of the concept in collective defence scenarios should remain NATO-centred. Otherwise, the Drone Wall may remain a politically visible but fragmented border surveillance project. If properly designed, however, it could evolve into a feasible defence layer that strengthens deterrence, force protection, and operational resilience against low-cost, high-volume, and hybrid unmanned threats on the eastern flank.

20.yıl | SETA

ANKARA • İSTANBUL • WASHINGTON D.C. • BERLİN • BRUSSELS

www.setav.org