ieee.es
Instituto Español de Estudios Estratégicos

Opinion
Paper



90/2026 11/09/2026

Guillem Colom Piella *

Escalating without crossing the threshold: Ukraine, the gray zone, and escalation management between Russia and NATO

Escalating without crossing the threshold: Ukraine, the gray zone, and escalation management between Russia and NATO

Abstract:

The war in Ukraine is progressively expanding in scope. Ukrainian strikes are reaching ever deeper into Russia's economic and logistical hinterland, while Moscow combines its campaign against Ukraine with an escalating gray-zone campaign across Europe. This interaction is blurring the boundary between the war in Ukraine and direct confrontation between Russia and NATO, increasing the risk of escalation. This Opinion Paper argues that the gray zone plays a particularly important role in this context: it allows coercion to be extended, costs imposed, and limits tested without resorting to overt military force. Yet this logic contains a contradiction. The more the gray zone is used to manage escalation, the greater the risk that it will erode the very thresholds it is intended to preserve.

Keywords:

Russia – Ukraine – NATO – gray zone – escalation – sabotage – coercion – deterrence

How to cite this document:

COLOM-PIELLA, Guillem. *Escalating without crossing the threshold: Ukraine, the gray zone, and escalation management between Russia and NATO*. Documento de Opinión IEEE 90/2026.

NOTE:** The views expressed in the ***Opinion Papers are those of the authors and do not necessarily reflect the views of the IEEE or the Ministry of Defence.

Introduction

The war in Ukraine is progressively expanding in scope. Without having become a war between Russia and NATO, several dynamics that could until now be analysed relatively separately are beginning to converge. Ukraine is carrying its strikes ever farther from the front line; Russia is increasing pressure on the Ukrainian rear while sustaining growing gray-zone activity on European soil; and the United States has in recent weeks resorted to different direct channels with Moscow and Kyiv to reduce the risk that these dynamics become coupled and to keep negotiations open. The result is a growing interaction between the war in Ukraine, gray-zone competition with the West, and deterrence between Russia and NATO.

This calls for renewed attention to the concept of escalation management. It does not mean controlling an interaction that also depends on the adversary's decisions and perceptions, but rather seeking to influence its intensity, scope, geography, and pace while preserving one's own options and constraining those of the opponent[1]. It also invites us to view the gray zone differently: not simply as a space between peace and war or as a catalog of hybrid instruments, but as an escalation-management regime – a framework that allows actors to compete, impose costs, test limits, and shift confrontation into other domains without accepting the risks of open war[2].

[1] It is useful to distinguish escalation management from escalation control. The former seeks to influence its direction, intensity, and pace without presuming an ability to determine the adversary's response. See KAHN, Herman. *On Escalation*. Praeger, 1965; SCHELLING, Thomas. *Arms and Influence*. Yale University Press, 1966; MORGAN, Forrest et al. Dangerous Thresholds. RAND, 2008.

[2] This interpretation develops the argument that the gray zone should be understood not as a simple space between peace and war, but as an escalation regime that fragments, calibrates, and redistributes coercion, shifts thresholds, and hinders the emergence of focal points capable of structuring a response. See COLOM-PIELLA, Guillem. “Desdibujar el umbral: zona gris, atribución y coerción acumulativa”. *Documento de Opinión del IEEE*, 47/2026, 30 April 2026. https://www.defensa.gob.es/ceseden/-/ieee/desdibujar-umbral-zona-gris-atribucion-y-coercion-acumulativa

A war expanding into strategic depth

The war continues to be decided on Ukrainian soil, but it has long ceased to be confined to the line of contact or its immediate rear. This expansion of the battlespace also cannot be separated from the difficulty of achieving decisive results on the ground. When the front offers few opportunities to alter the balance of forces quickly, long-range strikes become one of the domains in which both belligerents can still increase pressure, impose costs, and change the geography of the war.

Ukraine has been conducting a campaign of deep strikes against Russian territory for months. What is new is no longer that it can reach Russia, but the range of targets and their growing distance from the front line. Airfields, ammunition depots, bases, refineries, oil terminals, logistics infrastructure, industrial facilities and, more recently, large distribution centers now form part of an increasingly expansive battlespace.

The strikes on *Ust-Luga* and other energy facilities follow this logic. So too, although different in nature, do this summer's incidents involving *Wildberries* and *Ozon* logistics centers[3]. Not all these targets, however, perform a direct military function. The change lies in the broadening of the targeting process from military, energy, and industrial facilities to economic and logistics networks whose disruption also shifts the costs of the conflict into Russia. In doing so, Kyiv seeks to narrow the distance between front and rear, making the economic and material costs of the war more visible inside Russia.

Still, the deep-strike campaign should not be interpreted solely in terms of punishment. Faced with a shortage of interceptors, Ukraine is also trying to degrade Russian air

[3] *Reuters*, “Fire destroys drone-hit Wildberries warehouse in Russia's Tambov region, governor says”, 26 August 2026. https://www.reuters.com/world/drone-sets-wildberries-warehouse-ablaze-russias-tambov-region-governor-says-2026-08-26

defenses and locate the launchers generating missile salvos. Deep strikes therefore serve a coercive function, but also one of denial: they impose costs while seeking to reduce the adversary's capacity to continue attacking.

This is neither a new logic nor an exclusively Ukrainian development. Russia has conducted deep strikes since the outset of the invasion and, as early as the spring and summer of 2022, expanded its attacks against industrial facilities, fuel depots, logistics infrastructure, and other targets in Ukraine's rear[4]. From October onward, it also developed a systematic campaign against energy infrastructure. Its attacks on energy, industry, ports, logistics, and cities seek to degrade Ukraine's ability to sustain the war, but also to increase its economic, political, and social costs. The scale and density of these campaigns have nevertheless grown with the increasing combined use of drones and different types of missiles[5].

Yet greater destruction does not automatically translate into greater coercive leverage. Russia has spent years trying to convert damage to Ukrainian infrastructure and the population into political exhaustion without breaking Ukraine's will to fight. Nor is there yet evidence that the economic deterioration caused by Ukrainian strikes has substantially altered Putin's calculus. That gap between physical damage and political effect is central

[4] COLOM-PIELLA, Guillem. “Observaciones sobre el desempeño inicial de la Fuerza Aérea rusa en Ucrania”. *Revista de Aeronáutica y Astronáutica*, 926, pp. 768-773.

[5] Russia began the February 2022 invasion with a deep-strike campaign using ballistic and cruise missiles against air defenses, command and control, industrial facilities, and fuel and energy depots. From October that year, it also developed a systematic campaign against Ukraine's energy infrastructure. See ZABRODSKYI, Mykhaylo; WATLING, Jack; DANYLYUK, Oleksandr V. and REYNOLDS, Nick. *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022*. RUSI, 2022; WATLING, Jack and REYNOLDS, Nick. “Winter is Coming: Russia Turns to Countervalue Targeting”. *RUSI*, 1 November 2022. https://www.rusi.org/explore-our-research/publications/commentary/winter-coming-russia-turns-countervalue-targeting. As an indication of the scale reached, during the night of 26-27 August 2026 Russia launched a new wave of attacks across several Ukrainian regions involving 258 drones as well as ballistic and hypersonic missiles, striking, among other targets, port, energy, industrial, and logistics infrastructure.

to any escalation strategy: the parties can calibrate what they attack, but they cannot control the reaction they provoke[6].

This increase in pressure also coincided, in late August, with a period of negotiating deadlock. *Bloomberg* reported on 26 August that Moscow is considering intensifying its attacks and increasingly links Ukrainian deep strikes to the weapons and intelligence support provided by certain allied countries[7].

Nor does intensifying attacks contradict the prospect of eventual negotiations. In protracted wars, fighting continues while negotiations take place – or while each side seeks to improve the position from which it will eventually negotiate[8] – because military operations alter costs, expectations, and relative power. Both sides have incentives to demonstrate that time is hurting the adversary more than it is hurting them[9].

When deep strikes reach NATO's doorstep

The extension of the conflict is particularly sensitive in northwestern Russia, close to NATO territory. The Baltic region brings together several factors capable of turning a limited incident into an escalation problem: Ukrainian strikes against the Leningrad region, intense Russian electronic warfare activity, the proximity of Kaliningrad, deployed Allied forces, critical infrastructure, limited geographic depth, and a compressed airspace in which systems belonging to several actors operate.

[6] WALKER, Marcus. "The Russia-Ukraine Air War Has Entered a New, Deadlier Phase". *The Wall Street Journal*, 27 August 2026. https://www.wsj.com/world/the-russia-ukraine-air-war-has-entered-a-new-deadlier-phase-6d15cce1

[7] *Bloomberg*. "Putin Moves to Escalate War in Ukraine With Talks at Dead End", 26 August 2026. https://www.bloomberg.com/news/articles/2026-08-26/putin-moves-to-escalate-war-in-ukraine-with-talks-at-dead-end

[8] COLOM-PIELLA, Guillem. "Cómo terminan las guerras". *Documento de Opinión del IEEE*, 20 March 2025. https://www.defensa.gob.es/documents/2073105/2320887/como_terminan_las_guerras_2025_dieeeo20.pdf/e1c4dcf1-52bf-9ce1-f20f-23b29790f937?t=1742373675786

[9] On force and negotiation, see SCHELLING, *op. cit.*; SLANTCHEV, Branislav. "The Power to Hurt: Costly Conflict with Completely Informed States". *American Political Science Review*, 97(1), 2003, pp. 123-133.

Incidents have already occurred. On 14 August, a drone that entered Latvian airspace and was subsequently shot down was found to be Ukrainian. The Latvian Armed Forces considered it likely that Russian electronic warfare activity had diverted it[10]. This was not the first incident of its kind. The problem is less technical than political.

For Kyiv, it may simply be a weapon directed at a Russian target. For Riga or Tallinn, an accidental airspace incursion that has to be managed. For Moscow, however, it can become evidence – real or conveniently constructed – that Allied territory or airspace is being used to facilitate attacks on Russia.

That interpretation need not be correct to have strategic consequences. Escalation depends on actions, but also on the meaning each side assigns to them. This is where Russia's gray-zone campaign in Europe takes on another dimension.

From subversion to sabotage

Since the 2022 invasion, European countries have recorded a sharp increase in cyberattacks, interference, espionage, influence operations, reconnaissance of infrastructure, sabotage, arson, and other activities linked directly or indirectly to Russia.

The trend is becoming reasonably well documented, although any attempt at quantification must be treated cautiously because of attribution problems. The datasets compiled by the *Center for Strategic and International Studies* (CSIS) and the *International Institute for Strategic Studies* (IISS) show a sharp rise in these activities since 2022, their concentration on infrastructure, transport and industry, and the growing use of intermediaries recruited remotely[11].

[10] Ministry of Defence of Latvia. *The drone shot down in Balvi Municipality was a Ukrainian unmanned aerial vehicle*, 20 August 2026. https://www.mod.gov.lv/en/news/drone-shot-down-balvi-municipality-was-ukrainian-unmanned-aerial-vehicle

[11] JONES, Seth. "Russia's Shadow War Against the West", *CSIS*, 18 March 2025. https://www.csis.org/analysis/russias-shadow-war-against-west; EDWARDS, Charlie and

Using *proxies* reduces operational costs and complicates attribution, although employing poorly trained operatives also increases unpredictability. The incendiary parcels sent from Lithuania in 2024 are particularly illustrative. A joint investigation coordinated by Eurojust has identified twenty-two suspects allegedly connected to an operation carried out on behalf of Russian military intelligence. Several devices caught fire in Germany, Poland, and the United Kingdom. One began burning in Leipzig within the air-freight logistics chain[12].

The difference between starting a fire in a warehouse and having a similar device ignite aboard a cargo aircraft in flight is enormous, even if the instrument used is virtually the same. This is one of the central problems of escalation in the gray zone: small changes in target, timing, or circumstances can radically alter the consequences.

For this reason, the Leipzig episode deserves particular attention. In early August, a drone equipped with explosives and a detonator was found at Leipzig/Halle Airport, close to Ukrainian aircraft. Days later, another device carrying explosives was discovered, while a possible incident involving a cargo aircraft was also investigated. The case changed qualitatively in early September. On 1 September, the German government formally attributed the attempted attack to Russia, arguing that police investigations, the modus operandi, and intelligence findings pointed to Russian responsibility. German Interior

SEIDENSTEIN, Nate. *The Scale of Russian Sabotage Operations Against Europe's Critical Infrastructure*, IISS, 2025. https://www.iiss.org/research-paper/2025/08/the-scale-of-russian--sabotage-operations--against-europes-critical--infrastructure

[12] EUROJUST. *Joint investigation team disrupts group using self-igniting parcels for terrorist attacks*. Press Release, 6 March 2026. https://www.eurojust.europa.eu/news/joint-investigation-team-disrupts-group-using-self-igniting-parcels-terrorist-attacks. The joint investigation by Germany, Lithuania, the Netherlands, Poland, and the United Kingdom identified 22 suspects allegedly linked to Russian military intelligence. One of the devices sent from Lithuania in July 2024 caught fire in Leipzig shortly before it was to be loaded onto an aircraft.

Minister Alexander Dobrindt also stated that intelligence indicated that individuals involved had acted on behalf of Russian state agencies[13].

Estonia is also investigating a possible Russian connection to the fire at facilities used by Milrem Robotics, a supplier of unmanned systems to Ukraine[14].

The point is not to accumulate incidents or automatically attribute every accident in Europe to Russia. The key is to determine whether recognizable patterns in target selection, methods, and affected states emerge behind apparently disparate episodes.

Transport networks, railways, airports, the defense industry, communications, energy, logistics, and companies associated with support for Ukraine recur as targets. A recent study published by the *Hague Centre for Strategic Studies* (HCSS) argues precisely that this distribution is not random and that Russian pressure is concentrated especially on those states providing the greatest support to Ukraine. In this interpretation, sabotage and other gray-zone actions constitute a form of selective coercion intended to raise the political and material cost of sustaining Ukraine[15].

The gray zone as an escalation-management regime

The gray zone is often described through its instruments – cyberattacks, sabotage, disinformation, or covert action. For the present analysis, however, the catalog matters less than the logic linking those instruments: what they make possible.

[13] MARTINEZ, María. "Germany says Russia responsible for drone attack at Leipzig airport". 1 September 2026. https://www.reuters.com/world/europe/germany-says-russia-responsible-drone-attack-leipzig-airport-2026-09-01/

[14] *Reuters*. "Estonia PM says arson attack on defence contractor may be linked to Russia". 18 August 2026. https://www.reuters.com/business/aerospace-defense/estonia-pm-says-arson-attack-defence-contractor-may-be-linked-russia-2026-08-18

[15] IVEN, Markus; MANSFIELD, Ethan; EICHSTAEDT, Nicole and SWEEIJS, Tim. Europe's Strategic Trap: Why Russia's Sub-Threshold Coercion Is Succeeding and How to Stop It. *HCSS*, 30 June 2026. https://hcss.nl/report/europes-strategic-trap-why-russias-sub-threshold-coercion-is-succeeding-and-how-to-stop-it. The authors interpret sabotage, drone incursions, and other hybrid actions as a selective coercive strategy designed to raise the costs of European support for Ukraine.

One of its main advantages is that it allows aggression to be fragmented. An unambiguous conventional attack against an allied state presents a relatively recognizable political and military problem and, precisely for that reason, NATO deterrence is particularly robust against such a scenario. But effective deterrence against open military aggression does not necessarily eliminate coercion; it can displace it into domains where attribution is slower, the response less automatic, and consensus harder to achieve[16]. Pressure does not disappear; it changes form and level. Russia therefore has strong incentives to avoid an incident clear enough to facilitate Allied consensus on the need to respond.

Fragmentation alters that logic. A fire, railway sabotage, a drone incident, or a maritime episode with uncertain attribution may be insufficient on its own to justify a strategic response. Any one of them may appear insufficient; cumulatively, they can substantially alter the political calculus.

Hence the usefulness of understanding the gray zone as an escalation-management regime. It does not prevent escalation; rather, it allows escalation to be fragmented, distributed across domains, and modulated in intensity. Moscow can vary the type of action, the geography, the visibility of its involvement, and the damage inflicted without moving directly from political pressure to overt military force. It can also observe the Western reaction before deciding its next move.

The limitation is clear: Moscow can calibrate an action, but it cannot control the meaning the adversary assigns to it or the response it provokes. Even so, ambiguity, gradualism, and slow attribution give it considerable room for maneuver.

[16] HWANG, Ji-Jen. “Deterrence Bypass and the Erosion of Functional Authority: Rethinking Escalation in Grey-Zone Competition”. *Cogent Social Sciences*, vol. 12, 2026, https://www.doi.org/10.1080/23311886.2026.2675128.

The gray zone also makes it harder for a focal point capable of structuring the response to emerge. An unambiguous violation facilitates coordination because it allows actors to identify what has happened, which interest or norm has been breached, and why a response is necessary. Gradualism, ambiguity, and attribution problems do the opposite: each incident can be absorbed as an anomaly, crime, limited provocation, or isolated event[17].

This utility nevertheless contains a contradiction. By providing alternatives to the overt use of force, the gray zone can help contain escalation. Yet the more frequent, violent, or clearly attributable the actions become, the more they erode the threshold they were intended to preserve. In this sense, the gray zone can function simultaneously as a firewall and a transmission belt for escalation.

From Ukrainian strikes to their Western enablers

This logic becomes particularly important as Ukraine increases the reach and sophistication of its strikes against Russia. These operations depend to varying degrees on a broad set of enablers: intelligence, surveillance and reconnaissance, communications, navigation, technology, logistics, industrial support, and Western weapons. From the Allied perspective, there is a clear distinction between providing capabilities and participating directly in a combat operation. Moscow may not share that distinction.

The connection is no longer merely implicit. On 27 August, Russian Foreign Ministry spokesperson Maria Zakharova warned that British military facilities and equipment "…in

[17] On focal points as references that facilitate coordination in situations where actors must converge on a common option or expectation, see SCHELLING, Thomas. *The Strategy of Conflict*. Cambridge: Harvard University Press, 1960. On their application to thresholds and cumulative coercion in the gray zone, see COLOM-PIELLA, Guillem, *op. cit.*

Ukraine and beyond its borders" could become Russian targets in response to the use of British capabilities against Russian territory. The warning came after London announced that it would allow Kyiv access to classified technology to produce Storm Shadow missiles[18].

The statement does not necessarily announce an attack, but it makes explicit a relationship that had previously been more diffuse: a Ukrainian strike, a Western enabler, and a possible response against that enabler. Russia does not need to strike a British, German, or Polish military base with a missile in order to impose costs on the system sustaining Ukraine. It can act against a defense company, an airport, railway infrastructure, a logistics chain, or a communications network through sabotage, cyberattacks, proxies, or other covert actions.

The gray zone provides precisely that intermediate space: it allows some of the pressure associated with the increasing reach of Ukrainian strikes to be shifted toward Europe without yet bringing open war onto Allied territory. This does not retroactively turn every act of sabotage since 2022 into a response to Ukrainian deep strikes: Russia's campaign predates them and reflects a broader confrontation with the West. The question is whether, as Ukrainian operations reach farther into Russia, the pattern of sub-threshold targeting begins to shift toward the European enablers that make those operations possible.

Developments in early September point precisely in that direction. Denmark's Security Service has warned of concrete Russian preparations for sabotage against Danish defence companies and firms linked to military support for Ukraine. According to it,

[18] ANTONOV, Dmitry and OSBORN, Andrew. "Russia says it could strike UK military targets in response to Kyiv's use of British missiles". *Reuters*, 27 August 2026. https://www.reuters.com/world/europe/russia-says-it-could-strike-uk-military-targets-response-ukrainian-strikes-using-2026-08-27. Maria Zakharova warned that British military assets located in or outside Ukraine could become Russian targets if British systems continued to be used to strike Russian territory.

Russian intelligence services have also sought to recruit individuals remotely through social media and gaming platforms for apparently minor reconnaissance tasks, such as photographing companies or infrastructure, which could subsequently contribute to the preparation of sabotage operations[19].

When the firewall begins to fail

The risk increases when deeper Ukrainian strikes coincide with greater Russian strategic pressure, explicit threats against Western providers, and gray-zone activity increasingly close to Allied infrastructure.

A cyberattack, minor sabotage, or a fire causing no casualties can be handled through law enforcement, intelligence, sanctions, or public attribution. But when actions involve explosives, strike military facilities, or could cause mass casualties, the problem changes in nature.

There is no objective boundary indicating when a gray-zone campaign automatically becomes military aggression. That is precisely where its utility to the aggressor lies. But neither can that margin be assumed to be unlimited.

The accumulation of incidents, especially robust attribution, or a single episode with serious consequences can rapidly reconstruct the focal point that had previously remained blurred. An action causing mass casualties, an attack on critical military infrastructure, or an operation unambiguously linked to Russian services could change political perceptions of the campaign very quickly. The mechanism used to manage escalation may end up causing it.

[19] *Reuters*. "Russia recruits Danes for sabotage planning, Denmark says", 3 September 2026. https://www.reuters.com/world/russia-recruits-danes-sabotage-planning-denmark-says-2026-09-03/

The subsequent evolution of the Leipzig case also shows that reconstructing a focal point does not automatically entail crossing the threshold into a military response. German attribution transformed an initially ambiguous incident into an action politically attributed to Russia and facilitated coordination with allies, yet Berlin deliberately chose a diplomatic, economic, and security response that it presented as measured and proportionate. Attribution therefore reduced ambiguity without eliminating the scope for continued escalation management. The Russian reaction illustrates, at the same time, the limits of such calibration: measures conceived by one side as contained and proportionate can be interpreted – or deliberately portrayed – by the other as a further step up the escalation ladder

Washington and risk management

CIA Director John Ratcliffe's visit to Moscow in late August illustrates the problem well. Ratcliffe met in Moscow with senior Russian intelligence officials – Sergei Naryshkin has confirmed the meeting – and Putin was briefed afterward. Washington had informed Kyiv in advance and asked it temporarily to limit certain strikes while the U.S. delegation remained in Russia.

Subsequent reporting helps clarify the mission's significance. *The Wall Street Journal*, citing sources familiar with the mission, reports that Ratcliffe traveled to warn Russia against any attack on NATO member states. *CBS News* has independently corroborated the core of that account through several sources. According to these reports, U.S. assessments do not focus solely on a hypothetical conventional attack, but also on

cyberattacks, hybrid actions, provocations, or limited incursions designed to test Allied cohesion and the U.S. willingness to respond[20].

The reporting does not allow us to conclude that Russia has issued an ultimatum, decided to attack Estonia, or established an operational link between recent acts of sabotage and a specific military action. It does indicate, however, that Washington considers the risk of spillover into NATO serious enough to use a discreet channel at the highest level.

Subsequent contacts reinforce this interpretation. In early September, U.S. envoys Steve Witkoff and Jared Kushner travelled from Moscow to Kyiv in a renewed effort to restart negotiations. These contacts coincided with a temporary suspension of Russian strikes on Kyiv and Ukrainian strikes on Moscow, while fighting continued elsewhere and Ukraine maintained deep strikes against other Russian targets. Rather than a general de-escalation, the sequence suggests the deliberate limitation of particular actions in time and space in order to preserve room for negotiation without halting the war.

Conclusions

Deep strikes are carrying the war into Russia's economic and logistical rear; Western support makes the enablers sustaining those operations more visible; and Moscow's gray-zone campaign provides instruments for shifting some of that pressure toward Europe without yet accepting the costs of open military aggression.

[20] On the visit, see SELIGMAN, Lara; WARD, Alexander and DAWSEY, Josh. “CIA Chief's Surprise Moscow Trip Was to Warn Russia Not to Attack NATO”, *The Wall Street Journal*, 27 August 2026. https://www.wsj.com/politics/policy/cia-chiefs-surprise-moscow-trip-was-to-warn-russia-not-to-attack-nato-c2d997f3; GAZIS, Olivia and LAPORTA, James. “CIA Director John Ratcliffe warned Russia not to attack NATO during secretive trip”. *CBS News*, 27 August 2026. https://www.cbsnews.com/news/cia-john-ratcliffe-warned-russia-not-to-attack-nato-moscow-trip. Neither Washington nor Moscow has publicly confirmed the content of the warning.

That is both the strategic utility of the gray zone and its principal danger. It allows costs to be imposed, limits to be communicated, and tolerance to be tested while preserving a degree of ambiguity and reversibility. But as damage increases, ambiguity diminishes, and attribution becomes more robust, it becomes harder to continue treating each episode as an isolated event.

Europe cannot respond effectively either by treating each incident in isolation or by automatically attributing every accident, fire, or drone to Russia. It needs to reconstruct patterns, improve attribution, protect the enablers of support for Ukraine, and retain options for imposing costs before a serious incident ends up forcing a response. A purely reactive posture leaves the aggressor the initiative to decide when, where, and by what means to act.

The events of August and early September do not prove the existence of a single Russian plan. They do show that deep strikes, gray-zone pressure on Europe, Western enablers, and strategic management between Washington and Moscow are increasingly becoming part of the same escalation problem. Germany's attribution of the attempted Leipzig attack also shows how a reduction in ambiguity can transform an initially isolated incident into a focal point for political coordination and Allied response without necessarily crossing the threshold into open military confrontation.

The confrontation is progressively extending beyond Ukraine without yet becoming a war between Russia and NATO. The gray zone occupies precisely this intermediate space. It allows part of the confrontation to extend beyond the Ukrainian theater without yet bringing open war onto Allied territory. But the more it is used to manage escalation, the greater the risk of eroding the very limits it was intended to preserve. Understanding and managing that contradiction will remain one of the main challenges for European security for as long as the war continues.

*Guillem Colom Piella**
PhD in Security Studies
Adjunct professor at the Spanish Institute for Strategic Studies
@gcolpie