Documento
Opinión



90/2026 11 de septiembre de 2026

Guillem Colom Piella *

Escalar sin cruzar el umbral: Ucrania, zona gris y gestión de la escalada entre Rusia y la Alianza Atlántica

Escalar sin cruzar el umbral: Ucrania, zona gris y gestión de la escalada entre Rusia y la Alianza Atlántica

Resumen:

La guerra de Ucrania está ampliando progresivamente su alcance. Los ataques ucranianos penetran cada vez más en la profundidad económica y logística rusa, mientras Moscú combina su campaña contra Ucrania con una escalada en la zona gris sobre Europa. Esta interacción está haciendo menos nítida la frontera entre la guerra en Ucrania y una confrontación directa entre Rusia y la OTAN, aumentando con ello los riesgos de escalada. Este Documento de Opinión sostiene que la zona gris cumple aquí una función especialmente relevante: permite extender la coerción, imponer costes y probar límites sin recurrir a la fuerza militar abierta. Pero esta lógica contiene una contradicción. Cuanto más se utiliza para gestionar la escalada, mayor es el riesgo de erosionar los mismos umbrales que pretende preservar.

Palabras clave:

Rusia – Ucrania – OTAN – zona gris – escalada – sabotaje – coerción – disuasión

NOTA:** Las ideas contenidas en los ***Documentos de Opinión son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

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

Abstract:

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

Keywords:

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

Cómo citar este documento:

COLOM-PIELLA, Guillem. *Escalar sin cruzar el umbral: Ucrania, zona gris y gestión de la escalada entre Rusia y la Alianza Atlántica.* Documento de Opinión IEEE 90/2026.

Introducción

La guerra de Ucrania está ampliando progresivamente su alcance. Sin haberse convertido en una guerra entre Rusia y la Alianza Atlántica, varias dinámicas que hasta ahora podían analizarse de manera relativamente separada empiezan a aproximarse. Ucrania lleva sus ataques cada vez más lejos de la línea de frente; Rusia aumenta la presión sobre la retaguardia ucraniana y mantiene una creciente actividad en la zona gris sobre suelo europeo; y Estados Unidos ha recurrido en las últimas semanas a distintos canales directos con Moscú y Kiev para reducir el riesgo de que estas dinámicas terminen acoplándose y mantener abierta la negociación. El resultado es una interacción cada vez mayor entre la guerra en Ucrania, la competición en zona gris con Occidente y la disuasión entre Rusia y la OTAN.

Esto obliga a recuperar el concepto de gestión de la escalada. No significa controlar una interacción que depende también de las decisiones y percepciones del adversario, sino tratar de influir sobre su intensidad, alcance, geografía y ritmo, preservando al mismo tiempo las propias opciones y condicionando las del contrario[1]. Pero también invita a observar la zona gris de otra forma. No sólo como un espacio situado entre la paz y la guerra ni como un catálogo de instrumentos híbridos, sino como un régimen de gestión de la escalada: un marco que permite competir, imponer costes, probar límites y desplazar la confrontación hacia otros dominios sin asumir, necesariamente, los riesgos de una guerra abierta[2].

[1] Conviene distinguir gestión de control de la escalada. La primera busca influir sobre su dirección, intensidad y ritmo sin presuponer capacidad para determinar la respuesta adversaria. Véanse KAHN, Herman. *On Escalation*. Praeger, 1965; SCHELLING, Thomas. *Arms and Influence*. Yale University Press, 1966; MORGAN, Forrest et al. *Dangerous Thresholds*. RAND, 2008.

[2] Esta interpretación desarrolla el argumento de entender la zona gris no como una simple franja entre paz y guerra, sino como un régimen de escalada que fragmenta, dosifica y redistribuye la coerción, desplaza los umbrales y dificulta la aparición de puntos focales capaces de ordenar la respuesta. Véase COLOM-PIELLA, Guillem. "Desdibujar el umbral: zona gris, atribución y coerción acumulativa". *Documento de Opinión del IEEE*, 47/2026, 30 de abril de 2026. https://www.defensa.gob.es/ceseden/-/ieee/desdibujar-umbral-zona-gris-atribucion-y-coercion-acumulativa

Una guerra que se extiende hacia la profundidad del territorio

La guerra continúa decidiéndose en suelo ucraniano, pero hace tiempo que dejó de estar confinada a la línea de contacto o a su retaguardia inmediata. Esta ampliación del campo de batalla tampoco puede separarse de las dificultades para obtener resultados decisivos sobre el terreno. Cuando el frente ofrece pocas posibilidades de alterar rápidamente la relación de fuerzas, los ataques a largo alcance se convierten en uno de los ámbitos donde ambos contendientes todavía pueden aumentar la presión, imponer costes y modificar la geografía de la guerra.

Ucrania lleva meses desarrollando una campaña de ataques en profundidad contra territorio ruso. Lo novedoso ya no es que alcance Rusia, sino la variedad de objetivos y la creciente distancia respecto a la línea de frente. Aeródromos, depósitos de munición, bases, refinerías, terminales petroleras, infraestructuras logísticas, instalaciones industriales y, más recientemente, centros de distribución forman parte de un espacio de batalla cada vez más amplio.

Los ataques contra *Ust-Luga* y otras instalaciones energéticas siguen esta lógica. También lo hacen los episodios registrados este verano contra centros logísticos de *Wildberries* y *Ozon*[3]. Sin embargo, no todos estos objetivos tienen una función militar directa. El cambio está en la ampliación del proceso de selección de objetivos (*targeting*) desde instalaciones militares, energéticas o industriales hacia redes económicas y logísticas cuya disrupción traslada también los costes del conflicto al interior de Rusia.

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

Con ello, Kiev busca reducir la distancia entre el frente y la retaguardia, haciendo más perceptibles en el interior de Rusia los costes económicos y materiales de la guerra.

Sin embargo, no conviene interpretar la campaña de ataques en profundidad sólo en clave de castigo. Ante la escasez de interceptores, Ucrania también está intentando degradar las defensas aéreas rusas y localizar los lanzadores que generan las salvas de misiles. Los ataques en profundidad cumplen así una función coercitiva, pero también de negación: imponen costes y buscan reducir la capacidad adversaria de seguir atacando.

No es una lógica nueva ni una evolución exclusivamente ucraniana. Rusia ha realizado ataques en profundidad desde el comienzo de la invasión y, ya durante la primavera y verano de 2022, extendió sus ataques contra instalaciones industriales, depósitos de combustible, infraestructuras logísticas y otros objetivos situados en la retaguardia ucraniana[4]. A partir de octubre desarrolló, además, una campaña sistemática contra la infraestructura energética. Sus ataques contra energía, industria, puertos, logística y ciudades buscan degradar la capacidad de Ucrania para sostener la guerra, pero también aumentar sus costes económicos, políticos y sociales. La escala y densidad de estas campañas, sin embargo, han aumentado con el creciente empleo combinado de drones y misiles de distintos tipos[5].

[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] Rusia inició la invasión de febrero de 2022 con una campaña de fuegos en profundidad mediante misiles balísticos y de crucero contra defensas aéreas, mando y control, instalaciones industriales y depósitos de combustible y energía. Desde octubre de ese año desarrolló además una campaña sistemática contra la infraestructura energética ucraniana. Véanse ZABRODSKYI, Mykhaylo; WATLING, Jack; DANYLYUK, Oleksandr y REYNOLDS, Nick. *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022*. RUSI, 2022; WATLING, Jack y REYNOLDS, Nick. "Winter is Coming: Russia Turns to Countervalue Targeting". *RUSI*, 1 de noviembre de 2022. https://www.rusi.org/explore-our-research/publications/commentary/winter-coming-russia-turns-countervalue-targeting. Como muestra de la escala alcanzada, durante la noche del 26 al 27 de agosto, Rusia lanzó una nueva campaña de ataques contra distintas regiones ucranianas que incluyó 258 drones y misiles balísticos e hipersónicos, alcanzando infraestructuras portuarias, energéticas, industriales y logísticas.

Pero más destrucción no equivale automáticamente a mayor capacidad de coerción. Rusia lleva años intentando transformar el daño sobre las infraestructuras y la población ucranianas en agotamiento político sin haber quebrado su voluntad de lucha. Tampoco existe todavía evidencia de que el deterioro económico provocado por los ataques ucranianos haya modificado sustancialmente el cálculo de Putin. Esa distancia entre daño físico y efecto político es central para cualquier estrategia de escalada: las partes pueden graduar aquello que atacan, pero no controlar la reacción que provocan[6].

Este aumento de la presión coincidió, además, con un momento de estancamiento negociador. *Bloomberg* informó el 26 de agosto que Moscú contempla intensificar sus ataques y relaciona cada vez más los ataques en profundidad ucranianos con el armamento y el apoyo de inteligencia proporcionados por ciertos países aliados[7].

La intensificación de los ataques tampoco contradice una eventual negociación. En las guerras prolongadas se combate mientras se negocia – o mientras se intenta mejorar la posición desde la que se negociará[8] – porque las operaciones modifican costes, expectativas y poder relativo. Ambas partes tienen incentivos para demostrar que el paso del tiempo perjudica más al adversario que a ellas mismas[9].

[6] WALKER, Marcus. “The Russia-Ukraine Air War Has Entered a New, Deadlier Phase”. *The Wall Street Journal*, 27 de agosto de 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 de agosto de 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 de marzo de 2025. https://www.defensa.gob.es/documents/2073105/2320887/como_terminan_las_guerras_2025_dieeeo20.pdf/e1c4dcf1-52bf-9ce1-f20f-23b29790f937?t=1742373675786

[9] Sobre fuerza y negociación, 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.

Cuando la profundidad empieza a rozar la OTAN

La extensión del conflicto resulta especialmente delicada en el noroeste ruso, muy próximo al espacio aliado. El Báltico concentra varios factores capaces de convertir un incidente limitado en un problema de escalada: ataques ucranianos contra la región de Leningrado, intensa actividad rusa de guerra electrónica, la proximidad de Kaliningrado, fuerzas aliadas desplegadas, infraestructuras críticas, escasa profundidad geográfica y un espacio aéreo reducido en el que operan sistemas de varios actores.

Ya se han producido incidentes que muestran hasta qué punto esta proximidad puede generar problemas de escalada. El 14 de agosto, un dron ucraniano penetró en el espacio aéreo letón y fue posteriormente derribado. Según las Fuerzas Armadas letonas, lo más probable es que el aparato hubiese sido desviado de su trayectoria por la actividad rusa de guerra electrónica[10]. El episodio es relevante porque una operación dirigida inicialmente contra territorio ruso terminó afectando al espacio aéreo de un Estado aliado sin que existiera, aparentemente, intención ucraniana de hacerlo. No es el primer incidente de este tipo y, sobre todo, muestra que el problema no es únicamente técnico. Una desviación de navegación puede convertirse rápidamente en un problema político y estratégico cuando afecta a territorio aliado.

Para Kiev, puede tratarse simplemente de un vector dirigido contra un objetivo ruso. Para Riga o Tallin, de una intrusión accidental que debe ser gestionada. Para Moscú, en cambio, puede convertirse en evidencia – real o convenientemente construida – de que territorio o espacio aéreo aliado está siendo utilizado para facilitar ataques contra Rusia.

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

No es necesario que esa interpretación sea correcta para que tenga consecuencias estratégicas. La escalada depende de las acciones, pero también del significado que cada parte les atribuye. Y es ahí donde la campaña rusa de zona gris sobre Europa adquiere otra dimensión.

De la subversión al sabotaje

Desde la invasión de Ucrania, los países europeos han registrado un fuerte aumento de ciberataques, interferencias, espionaje, operaciones de influencia, reconocimiento de infraestructuras, sabotajes, incendios provocados y otras actividades vinculadas directa o indirectamente con Rusia.

La tendencia empieza a estar razonablemente documentada, aunque cualquier cuantificación debe tratarse con prudencia por los problemas de atribución. Las bases elaboradas por el *Center for Strategic and International Studies* (CSIS) y el *International Institute for Strategic Studies* (IISS) muestran un fuerte crecimiento de estas actividades desde 2022, su concentración sobre infraestructuras, transporte e industria y el creciente recurso a intermediarios reclutados a distancia[11].

El recurso a *proxies* abarata las operaciones y dificulta su atribución, aunque el empleo de ejecutores poco preparados aumenta también su imprevisibilidad. El caso de los paquetes incendiarios enviados desde Lituania en 2024 es especialmente ilustrativo. Una investigación conjunta coordinada por *Eurojust* ha identificado a veintidós sospechosos presuntamente relacionados con una operación realizada por cuenta de la inteligencia

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

militar rusa. Varios dispositivos ardieron en Alemania, Polonia y Reino Unido. Uno de ellos comenzó a arder en Leipzig dentro de la cadena logística aérea[12].

La diferencia entre provocar un incendio en un almacén y que un dispositivo similar se active dentro de un avión de carga en vuelo es enorme, aunque el instrumento empleado sea prácticamente el mismo. Éste es uno de los problemas centrales de la escalada en zona gris: pequeños cambios en el objetivo, el momento o las circunstancias pueden modificar radicalmente las consecuencias.

Por esta razón, el episodio de Leipzig merece especial atención. A comienzos de agosto apareció en el aeropuerto de esta localidad un dron equipado con explosivos y un detonador, mientras las autoridades investigaban otros aparatos y un posible incidente con un avión de carga. El caso experimentó, sin embargo, un cambio cualitativo a comienzos de septiembre. El Gobierno alemán atribuyó oficialmente a Rusia el intento de ataque, sosteniendo que la combinación de las investigaciones policiales, el patrón operativo y la información de inteligencia permitía identificar una responsabilidad rusa. Berlín señaló además que algunos de los implicados habrían actuado por cuenta de organismos estatales rusos. La atribución política se produjo mientras la investigación penal continuaba abierta[13].

Estonia investiga también una posible conexión rusa con el incendio de instalaciones utilizadas por *Milrem Robotics*, proveedor de sistemas no tripulados a Ucrania[14].

---

[12] *EUROJUST*. “Joint investigation team disrupts group using self-igniting parcels for terrorist attacks”. Press Release, 6 de marzo de 2026. https://www.eurojust.europa.eu/news/joint-investigation-team-disrupts-group-using-self-igniting-parcels-terrorist-attacks. La investigación conjunta de Alemania, Lituania, Países Bajos, Polonia y Reino Unido identificó a 22 sospechosos presuntamente relacionados con la inteligencia militar rusa. Uno de los dispositivos enviados desde Lituania en julio de 2024 ardió en Leipzig poco antes de ser cargado en un avión.

[13] MARTINEZ, María. “Germany says Russia responsible for drone attack at Leipzig airport”. *Reuters*. 1 de septiembre de 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 de agosto de 2026. https://www.reuters.com/business/aerospace-defense/estonia-pm-says-arson-attack-defence-contractor-may-be-linked-russia-2026-08-18

Lo importante no es acumular incidentes ni atribuir automáticamente a Rusia cualquier accidente ocurrido en Europa. La clave está en observar si, detrás de episodios aparentemente dispersos, aparecen patrones reconocibles en la selección de objetivos, los métodos empleados y los Estados afectados.

Transporte, ferrocarriles, aeropuertos, industria de defensa, comunicaciones, energía, logística y empresas relacionadas con el apoyo a Ucrania aparecen de manera recurrente. Un reciente estudio publicado por el *Hague Centre for Strategic Studies* (HCSS) sostiene precisamente que esta distribución no es aleatoria y que la presión rusa se concentra especialmente sobre aquellos Estados que proporcionan mayor apoyo a Ucrania. En esta interpretación, los sabotajes y demás acciones en zona gris constituyen una forma de coerción selectiva destinada a elevar el coste político y material de sostener a Ucrania[15].

La zona gris como régimen de gestión de la escalada

La zona gris suele describirse mediante sus instrumentos (ciberataques, sabotaje, desinformación o acciones encubiertas). Para este análisis, sin embargo, interesa menos el catálogo que la lógica que los articula: qué permiten hacer.

Una de sus principales ventajas es que permite fragmentar la coerción en acciones de menor entidad y más difícil atribución. Un ataque convencional contra un Estado aliado plantea un problema político y militar reconocible y, precisamente por ello, la disuasión aliada es especialmente efectiva frente a ese escenario. Pero una disuasión eficaz frente a un ataque armado abierto no elimina necesariamente la coerción; puede desplazarla

[15] IVEN, Markus; MANSFIELD, Ethan; EICHSTAEDT, Nicole y SWEEIJS, Tim. *Europe's Strategic Trap: Why Russia's Sub-Threshold Coercion Is Succeeding and How to Stop It*. HCSS, 30 de junio de 2026. https://hcss.nl/report/europes-strategic-trap-why-russias-sub-threshold-coercion-is-succeeding-and-how-to-stop-it/ Los autores interpretan los sabotajes, incursiones de drones y otras acciones híbridas como una estrategia coercitiva selectiva orientada a elevar los costes del apoyo europeo a Ucrania.

hacia formas de presión situadas por debajo de ese umbral, donde la atribución es más lenta, la respuesta menos automática y el consenso más difícil[16]. La presión no desaparece: cambia de forma y de nivel. Rusia tiene, por tanto, incentivos para evitar una acción suficientemente clara y grave como para facilitar el consenso aliado sobre la necesidad de responder.

La fragmentación altera esa lógica. Un incendio, un sabotaje ferroviario, un dron o un incidente marítimo de atribución dudosa pueden ser insuficientes por separado para justificar una respuesta estratégica. Por separado pueden parecer insuficientes; acumulados, pueden alterar sustancialmente el cálculo político.

De ahí que resulte útil entender la zona gris como un régimen de gestión de la escalada. No evita la escalada, sino que permite fragmentarla, distribuirla entre distintos dominios y modular su intensidad. Moscú puede variar el tipo de acción, la geografía, la visibilidad de su implicación y el daño producido sin pasar directamente de la presión política a la fuerza militar abierta. También puede observar la reacción occidental antes de decidir el siguiente movimiento.

Sin embargo, esta capacidad de gestión tiene un límite fundamental: Moscú puede graduar la acción, pero no controlar el significado que le atribuya el adversario ni la respuesta que provoque. Aun así, la ambigüedad, la gradualidad y la lentitud de la atribución le conceden un margen considerable.

La zona gris dificulta, además, la aparición de un punto focal capaz de ordenar la respuesta. Una violación inequívoca facilita la coordinación porque permite identificar qué ha ocurrido, qué interés o norma se ha vulnerado y por qué resulta necesario

[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.

reaccionar. La gradualidad, la ambigüedad y los problemas de atribución hacen justamente lo contrario: cada incidente puede ser absorbido como anomalía, delito, provocación limitada o hecho aislado[17].

Esta utilidad contiene, sin embargo, una contradicción. Al ofrecer alternativas al empleo abierto de la fuerza, la zona gris puede contribuir a contener la escalada. Pero cuanto más frecuentes, violentas o claramente atribuibles sean las acciones, más erosionan el umbral que pretendían preservar. En este sentido, la zona gris puede funcionar simultáneamente como cortafuegos y correa de transmisión de la escalada.

De los ataques ucranianos a sus habilitadores occidentales

Esta lógica adquiere especial importancia a medida que Ucrania aumenta la profundidad y sofisticación de sus ataques contra Rusia. Estas operaciones dependen en distinta medida de un amplio conjunto de habilitadores: inteligencia, vigilancia y reconocimiento, comunicaciones, navegación, tecnología, logística, apoyo industrial y armamento occidental. Desde la perspectiva aliada existe una diferencia clara entre proporcionar capacidades y participar directamente en una operación de combate. Moscú puede no compartir esa separación.

La asociación ya no es sólo implícita. El 27 de agosto, la portavoz del Ministerio de Exteriores ruso, Maria Zakharova, advirtió que instalaciones y equipos militares británicos en Ucrania y fuera de sus fronteras podrían convertirse en objetivos rusos en respuesta al empleo de capacidades británicas contra territorio ruso. La amenaza se

[17] Sobre los puntos focales como referencias que facilitan la coordinación en situaciones donde los actores deben converger sobre una opción o expectativa común, véase SCHELLING, Thomas. *The Strategy of Conflict*. Cambridge, Harvard University Press, 1960. Sobre su aplicación al problema de los umbrales y la coerción acumulativa en zona gris, véase COLOM-PIELLA, Guillem, *op. cit.*

produjo después de que Londres anunciara que permitiría a Kiev acceder a tecnología clasificada para producir misiles *Storm Shadow*[18].

La declaración no anuncia necesariamente un ataque, pero hace explícita una relación hasta ahora más difusa: ataque ucraniano, habilitador occidental y posible respuesta contra ese habilitador. Rusia no necesita atacar con un misil una base militar británica, alemana o polaca para imponer costes sobre el sistema que sostiene a Ucrania. Puede actuar sobre una empresa de defensa, un aeropuerto, una infraestructura ferroviaria, una cadena logística o una red de comunicaciones mediante sabotaje, ciberataques, *proxies* u otras acciones encubiertas.

La zona gris proporciona precisamente ese espacio intermedio: permite trasladar hacia Europa parte de la presión asociada al creciente alcance de los ataques ucranianos sin llevar todavía la guerra abierta al territorio aliado. Eso no convierte retrospectivamente todos los sabotajes desde 2022 en respuestas al ataque profundo ucraniano: la campaña rusa es anterior y responde a una confrontación más amplia con Occidente. La cuestión es si, a medida que aumenta el alcance de las operaciones ucranianas, el patrón de objetivos por debajo del umbral del conflicto abierto empieza a desplazarse hacia los habilitadores europeos que las hacen posibles.

Las informaciones aparecidas a comienzos de septiembre apuntan precisamente en esa dirección. El servicio de inteligencia danés ha advertido de preparativos concretos de sabotaje ruso contra empresas de la industria de defensa y compañías relacionadas con el apoyo militar a Ucrania. Según éste, parte de esta actividad incluye el

[18] ANTONOV, Dmitry y OSBORN, Andrew. “Russia says it could strike UK military targets in response to Kyiv's use of British missiles”. *Reuters*, 27 de agosto de 2026. https://www.reuters.com/world/europe/russia-says-it-could-strike-uk-military-targets-response-ukrainian-strikes-using-2026-08-27. Maria Zakharova advirtió que activos militares británicos situados dentro o fuera de Ucrania podrían convertirse en objetivos rusos si sistemas británicos continuaban empleándose para atacar territorio ruso.

reclutamiento a distancia de intermediarios para realizar tareas aparentemente menores de reconocimiento – como fotografiar empresas, infraestructuras o accesos – que pueden facilitar posteriormente acciones de sabotaje[19].

Cuando el cortafuegos empieza a fallar

El riesgo crece cuando coinciden una mayor profundidad de los ataques ucranianos, más presión estratégica rusa, amenazas explícitas contra los proveedores occidentales y una actividad en zona gris cada vez más próxima a infraestructuras aliadas.

Un ciberataque, un sabotaje menor o un incendio sin víctimas pueden gestionarse mediante instrumentos policiales, inteligencia, sanciones o atribución pública. Pero cuando las acciones incorporan explosivos, alcanzan instalaciones militares o pueden causar numerosas víctimas, el problema cambia de naturaleza.

No existe una frontera objetiva que indique cuándo una campaña de zona gris se convierte automáticamente en agresión militar. Precisamente ahí reside su utilidad para el agresor. Pero tampoco puede suponerse que ese margen sea ilimitado.

La acumulación de incidentes, una atribución especialmente sólida o un único episodio con consecuencias graves pueden reconstruir rápidamente el punto focal que hasta entonces había permanecido desdibujado. Una acción con numerosas víctimas, un ataque contra una infraestructura militar crítica o una operación inequívocamente vinculada con los servicios rusos podría cambiar en muy poco tiempo la percepción política de la campaña. El mecanismo utilizado para administrar la escalada puede terminar provocándola.

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

La evolución del caso de Leipzig muestra, además, que la reconstrucción del punto focal no implica necesariamente cruzar de manera automática el umbral de la respuesta militar. La atribución alemana transformó un incidente inicialmente ambiguo en una acción políticamente imputada a Rusia y facilitó la coordinación con los aliados, pero Berlín optó deliberadamente por una respuesta diplomática, económica y de seguridad que presentó como proporcionada y destinada a evitar una escalada mayor. La atribución redujo así la ambigüedad sin eliminar la posibilidad de seguir gestionando la escalada. La reacción rusa ilustra, al mismo tiempo, el límite de esa calibración: una respuesta concebida por una parte como proporcionada y contenida puede ser presentada por la otra como un nuevo peldaño de la escalada.

Washington y la gestión del riesgo

La visita a finales de agosto del director de la CIA, John Ratcliffe, a Moscú ilustra bien este problema. Ratcliffe se reunió en Moscú con responsables de los servicios de inteligencia rusos – Sergei Naryshkin ha confirmado el encuentro – y Putin fue informado posteriormente. Washington había avisado previamente a Kiev y pidió limitar temporalmente determinados ataques mientras la delegación estadounidense permanecía en Rusia.

Las informaciones publicadas posteriormente ayudan a entender mejor su alcance. *The Wall Street Journal*, citando fuentes conocedoras de la misión, sostiene que Ratcliffe viajó para advertir a Rusia contra cualquier ataque a Estados miembros de la OTAN. *CBS News* ha confirmado independientemente el núcleo de esa información mediante varias fuentes. Según estas informaciones, las evaluaciones estadounidenses no contemplan únicamente un hipotético ataque convencional, sino también ciberataques,

acciones híbridas, provocaciones o incursiones limitadas destinadas a probar la cohesión aliada y la voluntad estadounidense de responder[20].

La información no permite concluir que exista un ultimátum ruso, una decisión de atacar Estonia o una conexión operativa entre los sabotajes recientes y una acción militar concreta. Pero sí indica que Washington considera suficientemente serio el riesgo de extensión hacia la OTAN como para recurrir a un canal discreto a muy alto nivel.

La secuencia encaja con una lógica clásica de gestión de la escalada: mantener comunicación, señalar límites y reducir el riesgo de que una acción concreta desencadene una dinámica diferente de la buscada. La gestión estadounidense sugiere, en definitiva, que Washington empieza a tratar estos distintos planos como partes de un mismo problema de escalada.

Los contactos posteriores refuerzan esta interpretación. A comienzos de septiembre, los enviados estadounidenses Steve Witkoff y Jared Kushner viajaron de Moscú a Kiev en un nuevo intento de reactivar las negociaciones. Estos contactos coincidieron con una suspensión temporal de los ataques rusos contra Kiev y ucranianos contra Moscú, mientras continuaban las operaciones en otros sectores y los ataques en profundidad contra otros objetivos. Más que una desescalada general, la secuencia muestra una limitación deliberada de determinadas acciones, en tiempo y espacio, destinada a preservar margen para la negociación sin detener la guerra.

[20] Sobre la visita, véanse SELIGMAN, Lara; WARD, Alexander y DAWSEY, Josh. “CIA Chief's Surprise Moscow Trip Was to Warn Russia Not to Attack NATO”, *The Wall Street Journal*, 27 de agosto de 2026. https://www.wsj.com/politics/policy/cia-chiefs-surprise-moscow-trip-was-to-warn-russia-not-to-attack-nato-c2d997f3; GAZIS, Olivia y LAPORTA, James. “CIA Director John Ratcliffe warned Russia not to attack NATO during secretive trip”. *CBS News*, 27 de agosto de 2026. https://www.cbsnews.com/news/cia-john-ratcliffe-warned-russia-not-to-attack-nato-moscow-trip. Ni Washington ni Moscú han confirmado públicamente el contenido de la advertencia.

Conclusiones

Los ataques en profundidad llevan la guerra hacia la retaguardia económica y logística rusa; el apoyo occidental hace más visibles los habilitadores que permiten sostener esas operaciones; y la campaña en zona gris proporciona a Moscú instrumentos para trasladar parte de esa presión hacia Europa sin asumir todavía los costes de una agresión militar abierta.

Ahí reside la utilidad estratégica de la zona gris y también su principal peligro. Permite imponer costes, comunicar límites y probar tolerancias manteniendo cierto grado de ambigüedad y reversibilidad. Pero cuanto mayor sea el daño, menor la ambigüedad y más sólida la atribución, más difícil será seguir gestionando cada episodio como un hecho aislado.

Europa no puede responder adecuadamente ni atomizando cada incidente ni atribuyendo automáticamente a Rusia cualquier accidente, incendio o dron. Necesita reconstruir patrones, mejorar la atribución, proteger los habilitadores del apoyo a Ucrania y disponer de opciones para imponer costes antes de que un episodio grave termine obligando a responder. Una postura puramente reactiva deja al agresor la iniciativa para decidir cuándo, dónde y mediante qué instrumento actuar.

Los acontecimientos de agosto y comienzos de septiembre no prueban la existencia de un único plan ruso. Sí muestran que el ataque profundo, la presión en zona gris sobre Europa, los habilitadores occidentales y la gestión estratégica entre Washington y Moscú empiezan a compartir un mismo problema de escalada. La atribución alemana del intento de ataque de Leipzig muestra, además, cómo la reducción de la ambigüedad puede transformar un incidente inicialmente aislado en un punto focal para la coordinación política y la respuesta aliada sin que ello implique necesariamente cruzar el umbral de la confrontación militar abierta.

La confrontación se extiende progresivamente más allá de Ucrania sin haberse convertido todavía en una guerra entre Rusia y la OTAN. La zona gris ocupa precisamente ese espacio intermedio. Permite extender parte de la confrontación fuera del teatro ucraniano sin llevar todavía la guerra abierta al territorio aliado. Pero cuanto más se utiliza para administrar la escalada, mayor es también el riesgo de erosionar los límites que pretendía preservar. Entender y gestionar esa contradicción será uno de los principales retos para la seguridad europea mientras continúe la guerra.

*Guillem Colom Piella**
Doctor en Seguridad Internacional
Profesor asociado del IEEE
@gcolpie