Documento de Investigación

02/2026 22 de abril de 2026

Antonio Gil Fons y Saraí Valerdi Macías

La confrontación entre Rusia y la OTAN en la zona gris: hacia una necesaria toma de conciencia estratégica

La confrontación entre Rusia y la OTAN en la zona gris: hacia una necesaria toma de conciencia estratégica

Resumen:

El presente trabajo analiza la confrontación actual entre Rusia y la OTAN desde un enfoque neorrealista y de estudios de seguridad, sosteniendo que esta se desarrolla principalmente en la «zona gris», es decir, en un espacio de competencia estratégica por debajo del umbral del conflicto armado. A partir del caso ucraniano, se examina cómo Moscú ha perfeccionado durante más de dos décadas una panoplia de instrumentos híbridos —ciberataques, sabotajes, desinformación, apoyo a partidos y movimientos prorrusos, uso de *proxies* armados, coerción económica e interferencias en infraestructuras críticas— que hoy se proyectan sistemáticamente sobre países miembros de la OTAN. Esta dinámica erosiona el orden internacional, incrementa el riesgo de escaladas no deseadas y pone a prueba la seguridad nacional y colectiva aliada. Los mecanismos clásicos de disuasión, pensados para el conflicto convencional, son insuficientes. Se propone, por ello, una disuasión adaptada, que combine negación y represalia: fortalecimiento de la resiliencia —ciber, institucional y social—, coordinación interaliada, atribución pública, sanciones multisectoriales y una comunicación estratégica creíble. La tesis central es que solo una toma de conciencia estratégica y una disuasión eficaz en la zona gris pueden evitar que esta confrontación derive en una guerra convencional en Europa.

Palabras clave:

Zona gris, Rusia, OTAN, neorrealismo, disuasión.

The Russia–NATO Confrontation in the Gray Zone: Towards a Necessary Strategic Awareness

Abstract:

The present article analyzes the current confrontation between Russia and NATO from a neorealist and security studies perspective, arguing that it unfolds primarily in the "gray zone," that is, within a space of strategic competition below the threshold of armed conflict. Drawing on the Ukrainian case, it examines how Moscow has, for more than two decades, refined a panoply of hybrid instruments—cyberattacks, sabotage, disinformation, support for pro-Russian parties and movements, the use of armed proxies, economic coercion, and interference in critical infrastructures—which are now systematically projected against NATO member states. This dynamic erodes the international order, increases the risk of unintended escalation, and puts Allied national and collective security to the test. Classical deterrence mechanisms, designed for conventional conflict, are insufficient in this context. Accordingly, the article proposes an adapted form of deterrence combining denial and punishment: strengthening resilience —cyber, institutional, and societal—, enhancing inter-Allied coordination, public attribution, multisectoral sanctions, and credible strategic communication. The central thesis is that only strategic awareness and effective deterrence in the gray zone can prevent this confrontation from escalating into a conventional war in Europe.

Keywords:

Gray zone, Russia, NATO, Neorealism, Deterrence.

Cómo citar este documento:

GIL FONS, Antonio y VALERDI MACÍAS, Saraí. *La confrontación entre Rusia y la OTAN en la zona gris: hacia una necesaria toma de conciencia estratégica*. Documento de Investigación IEEE 02/2026. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

«El que desee la paz, así pues, ha de prepararse para la guerra». Las palabras escritas en el siglo IV por el romano Flavio Vegecio en su obra *Epitoma rei militaris* —con frecuencia resumidas como «si quieres paz, prepárate para la guerra»— siguen, en opinión de los autores, vigentes en la actualidad. El fin de la historia, proclamado por Fukuyama parece haber quedado atrás, y los dogmas asociados parecen estar superándose. El orden internacional y el Derecho Internacional son puestos en cuestión por poderosos actores, mientras que los mecanismos de cooperación multilateral o de diálogo se muestran ineficientes o incapaces. En un mundo que parece acumular dinámicas geopolíticas peligrosas, la Carta de las Naciones Unidas palidece ante el comportamiento, por acción o por omisión, de sus signatarios.

Desgraciadamente, en la última década se han producido varios hechos de los que es posible avergonzarse desde un punto de vista humano, moral, ético y legal. Ello obliga a impulsar profundas reflexiones, debates, consensos y mecanismos que impidan su repetición y las consecuencias derivadas. Un ejemplo claro de esto último se observa en el conflicto armado entre Rusia y Ucrania. Si bien este se inició oficialmente en febrero de 2022 con la invasión militar de Ucrania por parte de las fuerzas armadas rusas, durante las dos décadas anteriores se venía produciendo una confrontación no convencional entre Moscú y Kiev.

Este enfrentamiento, situado por debajo del umbral del conflicto armado internacional, y no regulado por el Derecho Internacional Humanitario, se caracterizó principalmente por el uso por parte de Moscú, de instrumentos híbridos frente a Ucrania en la denominada «zona gris». Así, durante años, Ucrania fue acosada mediante ciberataques, sabotajes, interferencias electorales, diplomacia coercitiva, presiones económicas, campañas de desinformación masiva, uso de grupos armados, etcétera. Esta estrategia híbrida de amplio espectro, desarrollada durante años, contribuyó a crear una situación favorable a la, en términos del Kremlin, «operación militar especial» iniciada en 2022 contra Ucrania.

El problema que se analiza en este texto es que las estrategias e instrumentos híbridos que durante dos décadas el Kremlin ordenó implementar y perfeccionar en Ucrania[1], están siendo reproducidos contra países miembros de la Organización del Tratado del

[1] En este trabajo, se entiende por estrategia híbrida el marco general de acción, mientras que los instrumentos híbridos constituyen los medios específicos —políticos, económicos, informativos, cibernéticos o militares— empleados para su ejecución.

Atlántico Norte (OTAN). En una acumulación de acciones cada vez más atrevidas, la zona gris entre Rusia y la OTAN ha adquirido nuevas dinámicas que pueden anteceder, tal y como ocurrió en el caso de Ucrania, a un conflicto armado internacional con características convencionales.

Este trabajo pretende responder a la pregunta de hasta qué punto las estrategias híbridas desplegadas por Rusia contra Ucrania, antes de 2022, están siendo reproducidas frente a países miembros de la OTAN, así como qué implicaciones tiene para la disuasión aliada. Ante la amenaza de verse arrastrada a una conflagración que quiebre lo que resta de paz en el Viejo Continente, los autores consideran que la OTAN, aun reconociendo las divergencias políticas internas que condicionan su capacidad de acción, ha de prepararse para el conflicto convencional, pero también para la confrontación que se desarrolla en la zona gris, ya que la disuasión efectiva en este ámbito es un elemento clave para evitar una nueva guerra. Y es que, recordando a Flavio Vegecio, si se quiere la paz, hay que prepararse para la guerra, incluida la confrontación en la zona gris.

Los hechos aquí recogidos no pretenden exhaustividad ni equivalencia causal, sino ilustrar patrones y mecanismos recurrentes. Se seleccionan y presentan priorizándolos por su relevancia estratégica, de modo que la evidencia sirva para una jerarquización analítica.

El trabajo se articula metodológicamente en un marco teórico neorrealista y de estudios de seguridad con el análisis de una selección de casos y episodios documentados en fuentes abiertas, informes especializados y literatura académica, desde un enfoque cualitativo. Los casos se eligen por su relevancia para ilustrar la proyección paulatina de los instrumentos híbridos rusos hacia el espacio de la OTAN, con el objetivo de identificar patrones de comportamiento y lógicas de confrontación en la zona gris. Cabe reconocer, no obstante, un sesgo analítico asumido, ya que, por razones de disponibilidad, verificabilidad y pertinencia, predominan fuentes euroatlánticas. Se considera que esta limitación no invalida los patrones identificados, pero sí se recomienda prudencia y una crítica racional.

El texto se divide en tres apartados. El primero de ellos es una aproximación teórico-conceptual a ciertos aspectos que deben considerarse en relación con el funcionamiento del sistema político internacional. Así, la teoría neorrealista de las relaciones

internacionales —como enfoque principal, pero no exclusivo— y los conceptos de seguridad nacional y de zona gris enriquecen el análisis.

El segundo apartado es una recopilación no exhaustiva de los instrumentos híbridos que el Kremlin ha venido empleando contra países miembros de la OTAN durante las dos últimas décadas. Su ejemplificación sirve para evidenciar una realidad: la confrontación entre Rusia y la OTAN más allá de Ucrania.

El tercer apartado se centra en la cuestión de la disuasión, profundizando en las complejidades que resultan de aplicar conceptos y mecanismos tradicionales a la zona gris, siendo ello fundamental para prevenir nuevos conflictos armados internacionales en el este de Europa.

Finalmente, las conclusiones cerrarán un texto que pretende invitar a la reflexión y a la toma de conciencia sobre las circunstancias geopolíticas actuales, con el objeto de superar las limitaciones de cómo nos gustaría que fuera el mundo y de promover que, en primer lugar, se piense en cómo es realmente. Con esta estructura, la presente investigación busca aportar un análisis sistematizado del uso de instrumentos híbridos por parte de Rusia contra la OTAN y su entorno, así como, a partir de la evidencia, proponer mecanismos de disuasión adaptados a la zona gris.

Neorrealismo en las relaciones internacionales, seguridad nacional y zona gris

El neorrealismo es una de las teorías con mayor desarrollo dentro de la siempre dinámica disciplina de las Relaciones Internacionales. Conceptualizado a finales de los años setenta por el estadounidense Kenneth Waltz, pretendió superar los límites de la teoría realista al introducir en el análisis el aspecto estructural del funcionamiento del sistema internacional[2]. En el nuevo enfoque propugnado por Waltz, el Estado continúa siendo el actor principal en las relaciones internacionales, pero el poder, fin último de la teoría realista, es ahora un instrumento para alcanzar el verdadero objetivo: la seguridad[3]. Para Waltz, «en situaciones cruciales […] la preocupación final de los Estados no es el poder,

[2] DE ALBA ULLOA, J. L. «Realismo estructural», en SCHIAVON, Jorge A. *et al.* (eds.), *Teorías de Relaciones Internacionales en el siglo XXI: Interpretaciones críticas desde México*. UABC, BUAP, UANL, UPAEP, 2014, pp. 227-249.
[3] Ibíd., pp. 227–249.

sino la seguridad»[4]. Ante este hecho, resulta necesario analizar «los eventos internacionales desde un nivel sistémico, en el que los actos de las grandes potencias —que son las unidades que interactúan dentro de la estructura— influyen en el resto de los Estados, dictando el orden y los equilibrios de fuerzas»[5]. Es decir, conviene estudiar tanto a los agentes como al sistema, el cual limita y condiciona el comportamiento de los primeros[6].

Según Waltz, el sistema tiene tres características fundamentales. La primera de ellas es la anarquía como principio ordenador. Con ello se refiere a la ausencia de una instancia supranacional que imponga a los Estados normas de comportamiento o que tenga una capacidad coercitiva superior —piénsese en las limitadas capacidades de la Organización de las Naciones Unidas o en la impune violación de numerosas resoluciones del Consejo de Seguridad—. Al no existir dicha instancia, los Estados son responsables de su propia seguridad[7].

«Cada Estado persigue sus propios intereses […] de la manera que juzgue mejor» y, ante la ausencia de una instancia conciliatoria en la que resolver sus diferendos o con capacidad coercitiva, «la fuerza es un medio para lograr los fines»[8], tal y como debió pensar el presidente ruso Putin en referencia a sus problemas con Ucrania. En esta anarquía, se favorece un entorno competitivo en el que prevalece el más fuerte[9], y en el que cualquier tipo de colaboración entre unidades —sea alianza, cooperación, distensión o incluso la paz— obedece a que las circunstancias de la estructura de la anarquía imperante y las capacidades e intereses de los Estados así lo requieren o convienen.

La segunda característica del sistema es que se compone de unidades con funciones similares, pero con diferentes capacidades, lo que repercute en las dinámicas internacionales que los Estados van a desarrollar y, en gran medida, en su posición

[4] WALTZ, Kenneth N. «The Origins of War in Neorealist Theory», *Journal of Interdisciplinary History*, 18 (4). 1988, pp. 615-628.
[5] DE ALBA ULLOA, J. L. «Realismo estructural», p. 243.
[6] KEOHANE, Robert O. *Instituciones internacionales y poder estatal: Ensayos sobre teoría de las relaciones internacionales*. Grupo Editor Latinoamericano, Buenos Aires, 1989; DE ALBA ULLOA, J. L. «Realismo estructural», en SCHIAVON, Jorge A. *et al.* (eds.), *Teorías de Relaciones Internacionales en el siglo XXI: Interpretaciones críticas desde México*. UABC, BUAP, UANL, UPAEP. 2014, pp. 227-249.
[7] TORO, Hugo. «Realismo y neorrealismo: ¿Una realidad superada?», *Revista de Marina*, 108 (805). 1991. Disponible en: https://revistamarina.cl/revistas/1991/6/toro.pdf; DE ALBA ULLOA, J. L. «Realismo estructural», en SCHIAVON, Jorge A. *et al.* (eds.). *Teorías de Relaciones Internacionales en el siglo XXI: Interpretaciones críticas desde México*. UABC, BUAP, UANL, UPAEP. 2014, pp. 227-249.
[8] WALTZ, Kenneth N. *Man, the State and War: A Theoretical Analysis*. Columbia University Press, New York, 1954.
[9] GAON, Federico. «Teoría de las Relaciones Internacionales y Medio Oriente: realismo» [entrada de blog]. 25 de junio de 2016. Disponible en: https://federicogaon.com/teoria-las-relaciones-internacionales-medio-oriente-realismo/

estructural. «Quienes mantienen las capacidades y el poder disponen de una amplia capacidad de tomar decisiones en política exterior»[10].

Finalmente, la tercera gran característica es el grado de concentración o difusión del poder, que define la polaridad del sistema: multipolar, bipolar, unipolar, unimultipolar, etc. El grado de concentración o difusión del poder no es inalterable en el tiempo, ya que varía de un sistema a otro y de una temporalidad a otra[11]. Las capacidades de poder constituyen el elemento variable de la estructura, cuyos cambios generan modificaciones en las dinámicas internacionales de cooperación y rivalidad[12].

En este escenario de anarquía y de competencia entre actores, se ha dado la paradoja de que un Estado —por ejemplo, Rusia—, al buscar fortalecer su seguridad —como en el caso de la invasión de Ucrania—, provoca un aumento de su inseguridad. Es lo que Herz denominó el dilema de la seguridad[13], según el cual, si bien un Estado puede interpretar —o argumentar— que su búsqueda de mayor poder se debe a cuestiones defensivas y de supervivencia, su entorno —la OTAN— puede percibir que dichas acciones responden a ambiciones ofensivas. «Cuando una gran potencia toma medidas para acrecentar su seguridad, de manera inversa decrece la seguridad de los demás —y se modifica el equilibrio de poder—»[14].

Frente a este problema, Waltz propugna un enfoque realista defensivo, en el que los Estados no deben buscar la maximización de su poder, pero sí mantener una cantidad adecuada para garantizar su supervivencia y adoptar decisiones racionales respecto de su acción exterior —«hacerlo porque es necesario»[15]—. En contraposición, Mearsheimer expone un realismo ofensivo en el que plantea que el Estado debe aprovechar cualquier oportunidad para obtener más poder, de modo que su maximización y la consecución de la hegemonía sean los objetivos fundamentales de la acción —«hacerlo porque se puede

[10] DE ALBA ULLOA, J. L. «Realismo estructural», pp. 231 – 232.
[11] KEOHANE, Robert O. *Instituciones internacionales y poder estatal.*
[12] KEOHANE, Robert O. *Instituciones internacionales y poder estatal: Ensayos sobre teoría de las relaciones internacionales*. Grupo Editor Latinoamericano, Buenos Aires, 1989; DE ALBA ULLOA, J. L. «Realismo estructural», en SCHIAVON, Jorge A. *et al.* (eds.), *Teorías de Relaciones Internacionales en el siglo XXI: Interpretaciones críticas desde México*. UABC, BUAP, UANL, UPAEP. 2014, pp. 227-249.
[13] HERZ, John H. *Political Realism and Political Idealism: A Study in Theories and Realities*. University of Chicago Press, Chicago, 1951.
[14] DE ALBA ULLOA, J. L. «Realismo estructural», p. 234.
[15] VARGAS, E. *El rol de Estados Unidos en el sistema político internacional de la posguerra fría* [tesis doctoral]. Universidad Complutense de Madrid, Instituto Universitario de Investigación Ortega y Gasset, Madrid, 2015.

hacer»[16]—. Sin embargo, estas propuestas responden más a la pregunta de cómo debería funcionar el sistema y no a la de cómo funciona. En cualquier caso, desde el neorrealismo se argumenta que el fin último que persiguen los Estados es la seguridad.

Sin duda, la seguridad nacional es un concepto clave y ordenador en la articulación de políticas nacionales e internacionales de numerosos Estados del mundo. No obstante, como bien señala Sagastegui[17], es «un concepto difícil de concebir y delimitar por la doctrina. […] Tiene márgenes muy amplios y una dependencia tan acusada de volátiles circunstancias», por lo que resulta sumamente compleja su definición. Para el general israelí Tal[18], «el concepto de seguridad nacional trata de salvaguardar la existencia de una nación y defender sus intereses vitales; la existencia es el objetivo básico de la seguridad». Por su parte, Laswell definió la seguridad nacional como «una ausencia de coerción procedente del exterior»[19]. Mientras tanto, Lustgarten y Leigh afirman que es «la defensa de la práctica democrática libre de manipulación extranjera, juntamente con la habilidad de defender la independencia de la nación y del territorio contra un ataque militar»[20].

Con el fin de la Guerra Fría, algunos académicos —Buzan[21]— superaron la visión tradicional —estatocéntrica— y propugnaron «una visión ampliada, destinada a preservar la seguridad de múltiples referentes, como son las personas vulnerables, los grupos étnicos y los gobiernos, entre otros», con la pretensión de incorporar al concepto otros tipos de amenazas como el cambio climático, la inseguridad alimentaria, la degradación medioambiental, el agotamiento de los recursos, etcétera[22]. Un ejemplo de esta visión ampliacionista se puede encontrar en España, donde, en el artículo 3 de la Ley de Seguridad Nacional, se define como «la acción del Estado dirigida a proteger la libertad, los derechos y el bienestar de los ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir, junto a

[16] Ibíd., p. 53.
[17] SAGASTEGUI, F. Y. *La seguridad nacional en el Estado constitucional de derecho* [tesis doctoral]. Universidad Carlos III de Madrid, Madrid, 2015.
[18] TAL, I. *National Security: The Israeli Experience*. Praeger Publishers, Westport, 2000.
[19] SAGASTEGUI, F. Y. *La seguridad nacional en el Estado constitucional de derecho*, p. 18.
[20] Ibíd., pp. 17 -18.
[21] BUZAN, Barry. *Introducción a los estudios estratégicos: Tecnología militar y relaciones internacionales*. Ediciones Ejército, Madrid, 1991.
[22] SAGASTEGUI, F. Y. *La seguridad nacional en el Estado constitucional de derecho*, p. 20.

nuestros socios y aliados, a la seguridad internacional en el cumplimiento de los compromisos asumidos»[23].

Del estudio de un significativo número de definiciones, ya sean tradicionales o ampliacionistas, se pueden extraer tres conclusiones: 1) el Estado es el garante de la seguridad nacional, ya que debe salvaguardar la soberanía nacional, el territorio y los derechos de sus ciudadanos, ya sea frente a amenazas internas o externas; 2) el concepto de seguridad nacional ha evolucionado —y lo sigue haciendo— con el tiempo; y 3) las definiciones de seguridad nacional, amenaza o intereses vitales poseen un carácter particular en cada país y sociedad, siendo el resultado de factores históricos, sociológicos, políticos, etcétera[24].

El objetivo primario de la seguridad nacional debe ser la salvaguarda de la existencia del Estado nación, ya que, al menos en los regímenes democráticos liberales, es un elemento clave y fundamental para garantizar el disfrute de los derechos por parte de la ciudadanía. Con base en esto, la mayor amenaza para la existencia de un Estado nación suele derivar de la existencia de un conflicto armado, ya sea de carácter internacional o no internacional. Sería lógico pensar que, en contraposición, la paz representa una situación idónea para la seguridad nacional. Sin embargo, una paz formal no implica necesariamente la ausencia de confrontación, dándose una serie de matices que configuran lo que se ha venido describiendo como un área volátil —«cambios frecuentes, rápidos y significativos»—, incierta —«los acontecimientos y los resultados son impredecibles»—, compleja —«multiplicidad de cuestiones y factores, algunos de los cuales pueden estar intrincadamente interconectados»— y ambigua —«entorno difuso en el que resulta complicado conocer la situación real—: la zona gris[25].

Si bien este concepto posee una larga trayectoria, ya que fue acuñado a principios de la Guerra Fría por pensadores como Kennan y recuperado con fuerza en la posguerra fría, su delimitación sigue siendo confusa. Habitualmente, se ha definido como una situación

[23] ESPAÑA. Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, *Boletín Oficial del Estado*, n.º 233. 29 de septiembre de 2015. Disponible en: https://www.boe.es/eli/es/l/2015/09/28/36 (consultado 11/3/2026).
[24] SAGASTEGUI, F. Y. *La seguridad nacional en el Estado constitucional de derecho.*
[25] SOTO SILVA, Julio. «La zona gris, un desafío para la conducción política y estratégica», *Cuadernos de Trabajo del Centro de Investigaciones y Estudios Estratégicos (ANEPE)*, n.º 6. 2021.

entre la guerra y la paz[26]. Sin embargo, Soto Silva[27] afirma que «un conflicto internacional en la zona gris se genera cuando […] los países que pretenden alterar el *statu quo* a su favor emplean estrategias multidimensionales y sincronizadas para minar gradualmente al adversario y lograr sus objetivos».

Por lo tanto, la zona gris no ha de ser entendida como un espacio entre la guerra y la paz, sino como un «mecanismo útil para forzar el *statu quo*» por parte de algunos actores estatales revisionistas en un entorno de competencia estratégica por debajo del umbral del conflicto armado[28]. En este sentido, el presente trabajo se distancia de las aproximaciones que entienden la zona gris como una mera situación transitoria entre la guerra y la paz. Así, los autores la conciben como un modo sostenido de competencia estratégica que se desarrolla de forma deliberada por debajo del umbral del conflicto armado, concepción que sirve como marco analítico para interpretar la relación Rusia–OTAN en las dos últimas décadas.

Las estrategias y tácticas que se desarrollan en la zona gris se caracterizan por la multidimensionalidad e hibridez de los métodos hostiles que emplean —desinformación, ciberterrorismo, sabotaje, apoyo a fuerzas irregulares no estatales, suma de pequeños hechos consumados, diplomacia coercitiva, disuasión militar, etcétera—. No llegan nunca a una confrontación armada directa —manteniéndose así en los márgenes del Derecho Internacional—, debido a la generación de acciones asimétricas frente a defensas convencionales —violación del espacio aéreo por drones—, a una ambigüedad que permite la negación plausible o la no atribución —uso de actores *proxy*—, y a la dificultad para cuantificar sus riesgos con base en modelos tradicionales. Esta ambigüedad dificulta la adopción de respuestas claras y coherentes, lo que favorece, en muchos casos, una escalada gradual de la confrontación —acciones de configuración del entorno, interferencia, desestabilización y empleo limitado y puntual de la fuerza—[29].

---

[26] JORDÁN, Javier. «El conflicto internacional en la zona gris», *Revista Española de Ciencia Política*, n.º 48. 2018, pp. 129-151. Disponible en: https://doi.org/10.21308/recp.48.05 (consultado 11/3/2026); SOTO SILVA, Julio. «La zona gris, un desafío para la conducción política y estratégica», *Cuadernos de Trabajo del Centro de Investigaciones y Estudios Estratégicos (ANEPE)*, n.º 6. 2021.

[27] SOTO SILVA, J. «La zona gris, un desafío para la conducción política y estratégica», p. 8.

[28] Ibíd., p.10.

[29] BAQUÉS, Josep. *Hacia una definición del concepto «Gray Zone» (GZ).* Documento de Investigación 02/2017, Instituto Español de Estudios Estratégicos, 2017; JORDÁN, Javier, «El conflicto internacional en la zona gris», *Revista Española de Ciencia Política*, n.º 48. 2018, pp. 129-151. Disponible en: https://doi.org/10.21308/recp.48.05 (consultado 11/3/2026); JORDÁN, Javier. «La disuasión en la zona gris: una exploración teórica», *Revista Española de Ciencia Política*, n.º 59. 2022, pp. 65-88; RODRÍGUEZ GÓMEZ, A. «Conflictos en la zona gris: la nueva amenaza

Así, el uso de acciones como la subversión política, la coerción económica, las operaciones de influencia sobre la opinión pública, los hechos consumados o las reivindicaciones de distinta naturaleza sobre otros Estados, «manteniendo a la propia sociedad como campo de batalla»[30], pueden lograr objetivos geopolíticos «que difícilmente se lograrían mediante una práctica política y jurídica de buena fe, pero sin tener que recurrir al empleo de la fuerza, de coste económico y social prohibitivo y siempre de consecuencias inciertas»[31]. Estas acciones pueden ser «suficientemente significativas como para desestabilizar regiones y afectar a la seguridad global»[32], lo que puede servir para «preparar a todos los niveles —social, ideológico, logístico, comunicativo, de obtención de inteligencia y, en ocasiones económico», el escenario para una futura guerra o, también, como instrumento de injerencia en las dinámicas posteriores a un conflicto armado[33].

Con base en todo lo anterior, es legítimo preguntarse por el fin último del recurso al uso de la zona gris por parte de Rusia frente a la OTAN. ¿Busca obtener réditos geopolíticos? ¿Busca generar condiciones para gestionar el posconflicto en Ucrania? ¿O acaso está preparando el escenario para una nueva y mayor guerra en Europa del Este? Desde una óptica liberal-institucionalista, estas dinámicas podrían interpretarse como un problema de insuficiencia de mecanismos de transparencia, verificación y gobernanza en la zona gris, en la que el coste de la acción oportunista es bajo y la atribución es difícil. Por su parte, un enfoque constructivista subrayaría el peso de narrativas identitarias, marcos históricos y percepciones mutuas de amenaza que facilitan la aceptación social de conductas revisionistas. Sin embargo, desde un marco neorrealista, la zona gris es el ámbito privilegiado en el que potencias revisionistas como Rusia intentan maximizar su seguridad y modificar el equilibrio de poder sin asumir los costes de un conflicto armado con la OTAN.

universal [Conflicts in the Gray Zone; The New Universal Threat]», *European Public & Social Innovation Review*, vol. 10. 2025, pp. 1-15. Disponible en: https://doi.org/10.31637/epsir-2025-1603 (consultado 11/3/2026); SOTO SILVA, J. «La zona gris, un desafío para la conducción política y estratégica», *Cuadernos de Trabajo del Centro de Investigaciones y Estudios Estratégicos (ANEPE)*, n.º 6. 2021.

[30] RODRÍGUEZ GÓMEZ, A. «Conflictos en la zona gris; la nueva amenaza universal [Conflicts in the Gray Zone; The New Universal Threat]», *European Public & Social Innovation Review*, vol. 10. 2025, pp. 1-15. Disponible en: https://doi.org/10.31637/epsir-2025-1603 (consultado 11/3/2026).

[31] SOTO SILVA, J. «La zona gris, un desafío para la conducción política y estratégica», p. 11.

[32] RODRÍGUEZ GÓMEZ, A. «Conflictos en la zona gris; la nueva amenaza universal», p. 2.

[33] BAQUÉS, J. *Hacia una definición del concepto «Gray Zone» (GZ),* pp. 15-16.

El presente trabajo adopta el neorrealismo como marco principal porque permite explicar mejor la lógica estructural de la competición, el dilema de la seguridad y el cálculo de costes y beneficios que incentiva el empleo sostenido de instrumentos híbridos por debajo del umbral del conflicto armado. Profundizar en la cuestión es importante, ya que el *Strategic Concept 2022* de la OTAN no utiliza el término «zona gris», aunque sí está presente su concepto de forma implícita cuando se refiere a amenazas híbridas o desafíos sistémicos[34]. Con dicho objetivo, el siguiente apartado expone algunos de los instrumentos híbridos que el Kremlin ha venido empleando contra países miembros de la OTAN durante las últimas décadas.

Instrumentos híbridos rusos en la zona gris en la confrontación con la OTAN

El colapso, desmembramiento y desaparición de la Unión Soviética durante el año 1991 dio paso a una Rusia con capacidades mermadas y raquíticas, enfrentada a severos problemas económicos, sociales, políticos y étnicos. Con un presidente Yeltsin en manos de los poderosos oligarcas —especialmente a medida que se deterioraba su salud—, la década de los años noventa fue traumática para el pueblo ruso, con humillaciones internas —derrota en la primera guerra de Chechenia (1994-1996)— y externas —bombardeo de su aliada Serbia en la guerra de Kosovo (1999)—. Por ello, desde su llegada al cargo de primer ministro el 9 de agosto de 1999 y, posteriormente, a partir del 31 de diciembre del mismo año, a la presidencia del país, Vladímir Putin trató de recuperar el orgullo nacional, cosechando una serie de éxitos en sus primeros años de mandato —superación de la crisis económica de finales de los noventa, victoria en la segunda guerra de Chechenia, subyugación de los oligarcas, etcétera—.

En el plano exterior, las capacidades del Estado ruso no podían compararse con las de Estados Unidos, la creciente Unión Europea o la emergente China, por lo que se recurrió de forma habitual al uso de instrumentos híbridos —menos costosos que los convencionales y más adaptativos a las nuevas realidades del siglo XXI— para fortalecer e incrementar su posición en el sistema político internacional de la posguerra fría, especialmente en el denominado «extranjero próximo», el espacio geopolítico

[34] NATO. *Strategic Concept 2022*. 2022, Disponible en: https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept (consultado 11/3/2026).

conformado por las antiguas repúblicas soviéticas y sus aledaños. Ucrania, si bien no es miembro de la OTAN, es, sin duda, el epítome del uso por parte de Rusia de instrumentos híbridos más allá de sus fronteras, por lo que merece ser analizada para ejemplificar las estrategias y acciones del Kremlin.

Ya durante el proceso electoral del año 2004, uno de los candidatos presidenciales, Viktor Yanukóvich, recibió un gran apoyo político y mediático por parte de Moscú, así como asesores. No obstante, la Revolución Naranja llevó a la presidencia de Ucrania al prooccidental Yúschenko, lo que hizo que, durante los siguientes años, el país sufriera presiones constantes por parte de Rusia, incluidas la confrontación por el precio del gas, la presión mediática y los ataques cibernéticos. Todo ello contribuyó al fracaso de la presidencia de Yúschenko, favoreciendo el triunfo electoral de Yanukóvich en las nuevas elecciones de 2010. El Kremlin parecía haber ganado la partida, pero el anquilosamiento del Estado ucraniano, la crisis multifactorial y la corrupción endémica, sumados a la polarización entre prooccidentales y prorrusos, llevaron a los acontecimientos de finales de 2013 y principios de 2014. Yanukóvich abandonó el país y se estableció un gobierno mucho más cercano a Bruselas que a Moscú. La reacción de Putin no se hizo esperar.

Durante la crisis política que azotaba a Ucrania, Rusia envió tropas adicionales a las bases que tenía en Crimea en virtud del Tratado de Partición de 1997[35]. Después, en febrero, soldados uniformados y armados, pero sin distintivos, argumentando ser milicias de autodefensa frente a Kiev, instalaron puestos de control en Armiansk y Chongar, los dos principales cruces de carretera entre la Ucrania continental y la península de Crimea[36]. De forma progresiva, estas supuestas milicias fueron ocupando las infraestructuras clave de la península. El resultado de estas acciones fue que la parte prorrusa de la zona consolidó el control territorial y operativo de los accesos e inició un proceso de separación e independencia. En marzo, aprovechando este escenario, se llevó a cabo el referéndum en el que se preguntó si querían que la República de Crimea se uniera a Rusia. De acuerdo con la Comisión Electoral, el 96,77 % de los votantes

[35] En 1997, un tratado integral entre Rusia y Ucrania afirmó la integridad de las fronteras ucranianas, algo que Rusia y las potencias nucleares occidentales también garantizaron en el *Memorando de Budapest* de 1994, cuando Ucrania acordó entregar su arsenal nuclear de fabricación soviética. Véase https://www.bbc.com/mundo/noticias-internacional-60237751 (consultado 11/3/2026).

[36] CUETO, José Carlos. «Rusia y Ucrania: así acabaron otras incursiones militares ordenadas por Putin», *BBC Mundo*. 6 de marzo de 2022, Disponible en: https://www.bbc.com/mundo/noticias-internacional-60524454 (consultado 11/3/2026).

estuvo a favor de la incorporación de este territorio a Rusia[37]. A raíz de ello, la Federación Rusa logró anexionarse Crimea, a pesar de la condena de la gran mayoría de la comunidad internacional.

El Kremlin también concentró su atención en Donetsk y Lugansk, provincias orientales de Ucrania pobladas mayoritariamente por ciudadanos de origen ruso asentados en el territorio en tiempos de Stalin. Los enfrentamientos entre unas autoproclamadas «milicias de autodefensa» y el ejército ucraniano llevaron a la implicación soterrada del Kremlin en el conflicto. Además del apoyo logístico, armamentístico y económico a las autoridades prorrusas rebeldes y a sus milicias, Rusia involucró de forma directa a miles de sus soldados profesionales —incluidas fuerzas especiales—, aunque siempre haciéndolos pasar por efectivos de las fuerzas locales. También existen pruebas de que dispuso sobre el terreno misiles antiaéreos portátiles y artillería pesada, así como otro tipo de armamento no convencional: los drones aéreos. Entre los modelos de los que se dotó a las fuerzas desplegadas en las provincias rebeldes se pudo observar el uso de los Granat-1 y -2, el ZALA-421–08, el Eleron 3SV y el Zastava[38]. El uso de este tipo de armamento permitió a los rebeldes apoyados por Moscú generar cuantiosas bajas en el bando ucraniano, mientras que se mantenían al mínimo las bajas separatistas.

Ucrania ilustra cómo una presión sostenida en la zona gris puede alterar los equilibrios estratégicos sin superar de forma explícita el umbral del conflicto armado. Así, la ambigüedad operativa reduce los costes esperados de la acción y dificulta la coordinación del disuasor, mientras que, desde la óptica del realismo ofensivo, estas prácticas maximizan las ganancias oportunistas en ventanas temporales favorables. Este patrón es relevante porque anticipa la lógica del uso de instrumentos híbridos en entornos en el que el adversario sí posee compromisos de defensa colectiva.

Además de la confrontación armada que Rusia impulsaba de forma más o menos velada en el este de Ucrania, entre los años 2014 y 2022 se produjeron una serie de ataques no convencionales cuya autoría apunta al Kremlin. En 2014, el *malware* de ciberespionaje Snake —también conocido como Ouroboros— atacó e infectó numerosas

[37] BONET, P. «Crimea se abraza a la Rusia de Putin», *El País*. 16 de marzo de 2014. Disponible en: https://elpais.com/internacional/2014/03/16/actualidad/1394974142_352878.html (consultado 11/3/2026).
[38] JORDÁN, J. «Algunas lecciones del combate terrestre en el Dombás», *Global Strategy*. 2019. Disponible en: https://global-strategy.org/algunas-lecciones-del-combate-terrestre-en-el-donbass-2014-2015-artilleria-fuerzas-acorazadas-y-mecanizadas/ (consultado 11/3/2026).

redes informáticas en Ucrania. Este *malware* resultó ser muy similar a uno que anteriormente había atacado los sistemas del Pentágono estadounidense. De hecho, el virus Snake también atacó en Lituania, Reino Unido y Georgia[39]. En 2016, se efectuó con éxito un ciberataque que dejó sin electricidad durante una hora a Kiev. Este ciberataque fue ejecutado mediante *spear phishing* —ingeniería social— y, según el Departamento de Seguridad Nacional de Estados Unidos, aproximadamente 80.000 clientes de la empresa de servicios públicos Prykarpattyaoblenergo resultaron afectados en el oeste de Ucrania[40].

El hecho demostró las vulnerabilidades de Ucrania frente a este tipo de ataques cibernéticos, cuyos beneficios en el siglo XXI pueden ser mucho mayores que sus costes mínimos. De hecho, ya en 2007, Estonia, tras la retirada de un monumento de la época soviética, había sufrido una oleada de ciberataques DDoS —ataques distribuidos de denegación de servicio— que buscaron saturar los sistemas de bancos, ministerios, medios y del Parlamento[41]. En 2015, un ciberataque bloqueó las transmisiones de varios canales de TV5Monde. Si bien en un inicio fue reivindicado por un supuesto grupo yihadista, investigaciones posteriores del Gobierno francés atribuyeron el ataque al GRU —inteligencia militar— de Rusia. También en ese mismo año se detectó una penetración no autorizada en la red del Parlamento alemán, de la cual se acusó a un miembro de APT28, grupo de *hackers* vinculados al GRU.

Por otra parte, los servicios de inteligencia checos y búlgaros acusaron al GRU — inteligencia militar de Rusia— de ser el responsable de las explosiones que se produjeron en sendos depósitos de municiones en Chequia y Bulgaria entre 2014 y 2015, con el objetivo de obstaculizar el suministro de armas a Ucrania.

El objetivo estratégico no es únicamente influir en decisiones puntuales, sino en erosionar la cohesión de los países miembros de la OTAN y aumentar su incertidumbre interna. Si se perciben costes políticos y sociales crecientes por sostener una postura firme, la capacidad de coordinación disminuye y la disuasión se degrada. Dicho de otro

[39] SANGER, D. y ERLANGER, S. «Suspicion falls on Russia as cyberattacks target Ukraine», *The New York Times*. 9 de marzo de 2014, Disponible en: https://www.nytimes.com/2014/03/09/world/europe/suspicion-falls-on-russia-as-snake-cyberattacks-target-ukraines-government.html (consultado 11/3/2026).
[40] BBC NEWS. «Hackers causaron un corte de electricidad en el oeste de Ucrania, según EE. UU.», *BBC*. 12 de enero de 2016. Disponible en: https://www.bbc.com/news/technology-35297464 (consultado 11/3/2026).
[41] GRASSEGER, Hannes y KROGERUS, Mikael. «Fake news, botnets and how Russia weaponised the web», *The Guardian*. 2 de diciembre de 2017. Disponible en: https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia (consultado 11/3/2026).

modo, la lógica de la zona gris no reside en la obtención de victorias decisivas, sino en la acumulación progresiva de costes políticos, sociales y estratégicos para el adversario.

Con base en lo anterior, es destacable el apoyo directo o indirecto que desde el Kremlin se ha dado a una serie de partidos políticos en Europa, tales como la actual Agrupación Nacional —anteriormente Frente Nacional— de Marine Le Pen en Francia, AfD en Alemania, la Lega en Italia, el FPÖ en Austria, Fidesz en Hungría, etcétera[42]. Diversas investigaciones parlamentarias y periodísticas han denunciado tramas de financiación irregular de miembros de dichas formaciones, vínculos con enviados del Kremlin y una presencia constante en medios de comunicación prorrusos.

También es de destacar las campañas híbridas llevadas a cabo en Europa báltica y central, en las que fuerzas euroescépticas han recibido un apoyo constante a través de empresas y sociedades vinculadas al Kremlin[43].

Durante la campaña de las elecciones estadounidenses de 2016, una serie de sucesos parecían ir en el sentido de favorecer al candidato presidencial republicano: el hackeo y posterior filtración de correos electrónicos del Comité Nacional Demócrata y de la campaña de Hillary Clinton, el uso de plataformas como WikiLeaks para difundir selectivamente información dañina, así como el uso masivo de bots y trolls en redes sociales para amplificar contenidos en favor de uno de los candidatos y polarizar la campaña[44].

En 2016, las fuerzas de seguridad de Montenegro, en aquel momento candidato a la OTAN, desarticularon el día de las elecciones un complot para asaltar el Parlamento, matar al primer ministro e instaurar un gobierno prorruso tras las elecciones parlamentarias. Los tribunales condenaron a varios ciudadanos montenegrinos y a agentes rusos. En 2016, en Moldavia, el prorruso Igor Dodon, del Partido de los

[42] BOYLE, Catherine. «Russian links to EU far right exposed by French loan», *CNBC*. 25 de noviembre de 2014. Disponible en: https://www.cnbc.com/2014/11/25/russian-links-to-eu-far-right-exposed-by-french-loan.html (consultado 11/3/2026); PABST, Stefan. «Is the Kremlin financing Europe's right-wing populists?», *DW*. 29 de noviembre de 2014. Disponible en: https://www.dw.com/en/is-the-kremlin-financing-europes-right-wing-populists/a-18101352 (consultado 11/3/2026).

[43] EUVSDISINFO. «Las mentiras de la Plaza Roja: propaganda en el desfile, en Internet y en las calles», *EUvsDisinfo*. 8 de mayo de 2025. Disponible en: https://euvsdisinfo.eu/es/las-mentiras-de-la-plaza-roja-propaganda-en-el-desfile-en-internet-y-en-las-calles/ (consultado 11/3/2026).

[44] ACKERMAN, S., THIELMAN, S. y SMITH, D. «US intelligence report: Vladimir Putin 'ordered' operation to get Trump elected», *The Guardian*. 6 de enero de 2017. Disponible en: https://www.theguardian.com/world/2017/jan/06/vladimir-putin-us-election-interference-report-donald-trump (consultado 11/3/2026).

Socialistas (PSRM), se impuso en las elecciones presidenciales. A continuación, visitó Moscú. Desde esa fecha, Rusia, a través de GRU y el FSB, ha financiado al PSRM y a redes prorrusas en el país y ha utilizado fondos para campañas y protestas.

En 2017, poco antes de la segunda vuelta de las elecciones presidenciales francesas, se produjo un robo y la filtración masiva de documentos de la campaña de Emmanuel Macron. Diversas investigaciones señalaron la implicación del grupo APT28, vinculado al GRU. Durante toda la década del 2010, Rusia invitó y apoyó a los líderes del UKIP y de fuerzas euroescépticas, lo que les otorgó un notable protagonismo en medios de comunicación internacionales afines al Kremlin, como RT o Sputnik. Se fomentaron narrativas alineadas con el Brexit, la oposición a las sanciones contra Rusia y las críticas a la OTAN[45].

En 2018, Serguéi Skripal, un antiguo espía ruso, y su hija sufrieron un ataque con el agente nervioso conocido como Novichok. Se acusó de ello a agentes del GRU. El Kremlin reaccionó con una campaña masiva de desinformación en medios y redes sociales. En 2018, durante el ejercicio Trident Juncture de la OTAN, Noruega y Finlandia denunciaron interferencias deliberadas en el sistema GPS, responsabilizando a Rusia de una maniobra de guerra electrónica que podía afectar desastrosamente a la aviación civil.

La unidad EUvsDisinfo y el Servicio Europeo de Acción Exterior han documentado centenares de campañas de desinformación masiva que tratan de influir en las opiniones públicas de los países miembros de la OTAN, ya sea en temas referidos a elecciones nacionales, referéndums, debates, percepción de Rusia, migración, valores, vacunas, etcétera[46].

En 2022, Kiev denunció que un grupo llamado *Sandworm* desplegó programas maliciosos para destruir y borrar datos en los ordenadores que controlan las subestaciones de alta tensión en Ucrania[47]. A pesar de que este ataque no fue exitoso como el de 2016, la Federación Rusa logró generar incertidumbre en la población y preparar el terreno para una nueva fase del conflicto. En febrero de 2022, Putin,

[45] BOYLE, C. «Russian links to EU far right exposed by French loan».
[46] EUVSDISINFO. «Las mentiras de la Plaza Roja: propaganda en el desfile, en Internet y en las calles».
[47] REUTERS. «Hackers rusos intentaron sabotear la red eléctrica ucraniana -autoridades e investigadores», *Euronews*. 12 de abril de 2022. Disponible en: https://es.euronews.com/2022/04/12/ucrania-crisis-ciber

insistiendo en que no se trataba ni de una guerra ni de una invasión**,** sino que era una «operación militar especial» para defender a la población rusófona y desnazificar el país vecino y, en el marco de una amplia estrategia híbrida de comunicación, desinformación y ciberataques, ordenó la invasión de Ucrania[48].

Con el inicio de la invasión rusa de Ucrania en febrero de 2022, el Kremlin combinó estrategias propias de la guerra convencional con instrumentos híbridos en una campaña de amplio espectro destinada no solo a subyugar al pueblo ucraniano, sino también a disuadir o dificultar cualquier posible ayuda externa a Kiev. En el primer caso, el ataque sistemático y periódico con misiles y drones rusos contra centrales y subestaciones eléctricas ucranianas —infraestructura civil—, especialmente a partir del otoño de 2022, con la finalidad de dejar sin luz a la población no combatiente de cara al invierno, constituye sin duda una violación clara del Derecho Internacional Humanitario. Por otra parte, se han denunciado ataques constantes de *malware* —WhisperGate, HermeticWiper, variantes de Sandworm— contra ministerios, bancos e infraestructuras críticas.

En referencia a la campaña híbrida contra países miembros de la OTAN y de la UE, entre 2022 y 2025 se han detectado alrededor de ciento cincuenta incidentes en infraestructuras —explosiones menores, incendios sospechosos, sabotajes de ferrocarriles, cables submarinos cortados, etcétera— que las autoridades europeas han atribuido a actores vinculados al Kremlin o a sus *proxies*, lo que ha supuesto una distracción significativa de recursos por parte de los países afectados.

Moldavia, país que alberga a más de mil soldados rusos estacionados en la disputada región de Transnistria, ha sido uno de los objetivos preferidos de las estrategias híbridas de Rusia. Investigaciones realizadas por parte de RISE Moldova/OCCRP han denunciado la existencia de una red de financiación rusa que da apoyo a figuras prorrusas como Igor Dodon, quien fue presidente del país entre 2016 y 2020, así como a partidos políticos afines como el PSRM o el Partido Șor. Además, esta financiación

[48] CUETO, J. C. «Rusia y Ucrania: así acabaron otras incursiones militares ordenadas por Putin», *BBC*. 6 de marzo de 2022. Disponible en: https://www.bbc.com/mundo/noticias-internacional-60524454 (consultado 11/3/2026); *EL PAÍS*. «¿Cuál es el origen del conflicto entre Rusia y Ucrania?», *El País*. 1 de marzo de 2022. Disponible en: https://elpais.com/internacional/2022-03-01/origen-del-ataque-de-rusia-a-ucrania.html (consultado 11/3/2026).

habría servido también para pagar la compra de votos e incitar protestas antigubernamentales y antieuropeas[49].

En 2023, el Partido Șor, liderado desde Moscú por el oligarca prófugo Ilan Shor, fue ilegalizado por el Tribunal Constitucional de Moldavia, al considerarlo un instrumento ruso para hacerse con el control del Estado moldavo y frenar su acercamiento a la Unión Europea. En 2025, Yevgenia Gutsul, una de las líderes del Partido Șor, fue condenada a siete años de cárcel por introducir de forma ilegal dinero desde Rusia para financiar tanto a su formación política como para la organización de protestas prorrusas[50].

Además, durante las elecciones presidenciales de 2024 y las parlamentarias de 2025, según denunciaron las autoridades y la inteligencia moldava, proliferaron ciberataques, campañas de desinformación en redes sociales populares, la compra de votos, la financiación de partidos prorrusos e intentos de protestas violentas contra el gobierno proeuropeo de Maia Sandu[51]. Además, a las formaciones políticas Moldova Mare y Partidul Republican «Inima Moldovei» se les impidió participar en las elecciones legislativas de 2025 bajo la acusación de haber sido financiadas ilegalmente desde el extranjero[52].

También hay que destacar el complejo caso de Rumanía. Desde el año 2023, EUvsDisinfo y otros observatorios han venido documentando campañas masivas que tratan de imponer en redes sociales narrativas prorrusas, ya sea mediante la relativización de la agresión rusa a Ucrania, la difamación de la UE y de la OTAN, los

[49] MCGRATH, S. «Moldova election raids point to Russian interference», *Associated Press*. 23 de septiembre de 2025. Disponible en: https://apnews.com/article/moldova-election-russia-raids-europe-8f32d48131335f44be2bb5f5d55f934d (consultado 11/3/2026); ROBERT LANSING INSTITUTE. «The Kiriyenko blueprint: Turning Moldova's election into an operation», *Robert Lansing Institute*. 25 de septiembre de 2025. Disponible en: https://lansinginstitute.org/2025/09/25/the-kiriyenko-blueprint-turning-moldovas-election-into-an-operation/ (consultado 11/3/2026).

[50] SAUER, P. «Moldovan regional leader sentenced to seven years in prison over Russian funding», *The Guardian*. 5 de agosto de 2025. Disponible en: https://www.theguardian.com/world/2025/aug/05/moldova-gagauzia-yevgenia-gutsul-sentenced (consultado 11/3/2026).

[51] MCGRATH, S. y GHIRDA, V. «Moldova presidential election marred by corruption and fraud allegations», *Associated Press*. 3 de noviembre de 2024. Disponible en: https://apnews.com/article/moldova-presidential-election-russia-corruption-fraud-5886447779a4a818e9f30fdadcb8bbe5 (consultado 11/3/2026); PRESS ROOM. «Russia intensifies disinformation campaign targeting Moldovan parliamentary elections», *DISA*. 22 de septiembre de 2025. Disponible en: https://disa.org/russia-intensifies-disinformation-campaign-targeting-moldovan-parliamentary-elections/ (consultado 11/3/2026).

[52] CAMINO, J. «Moldova bans pro-Russia party from parliamentary elections», *DW*. 26 de septiembre de 2025. Disponible en: https://www.dw.com/en/moldova-bars-pro-russia-party-from-parliamentary-elections/a-74153073 (consultado 11/3/2026); REUTERS. «Kremlin denies interference in Romanian election», *Reuters*. 29 de noviembre de 2024. Disponible en: https://www.reuters.com/world/europe/kremlin-denies-russian-interference-romanian-election-2024-11-29/ (consultado 11/3/2026).

insultos a candidatos proeuropeos, etcétera[53]. El apogeo de esta campaña llegó durante las elecciones presidenciales de 2024, cuando Călin Georgescu, candidato nacionalista, antieuropeo y prorruso, se impuso por sorpresa en la primera vuelta tras una intensa presencia de sus mensajes en redes sociales como TikTok y Telegram. Poco después, desde los servicios de seguridad rumanos y desde medios internacionales se denunció que la candidatura de Georgescu había sido apoyada por una operación masiva de desinformación y manipulación coordinada desde Rusia, recurriéndose a un uso intensivo de bots, cuentas falsas y contenidos virales. Esto llevó a que la Corte Constitucional anulara los resultados al llegar a la conclusión de que hubo una injerencia extranjera significativa, mediante operaciones cibernéticas, uso de bots en redes sociales, financiación irregular, etcétera[54].

Las acciones rusas también se han dejado sentir en otros países miembros de la OTAN. Así, seis ciudadanos extranjeros están acusados en Lituania de, por encargo del GRU, haber intentado atentar en 2024 contra la empresa TVC Solutions, proveedora de las Fuerzas Armadas ucranianas. Además, se sospecha de su implicación en ataques e intentos de ataques contra autobuses, una oficina de correos, centros comerciales, un cine, un almacén de papel e infraestructuras petroleras y gasísticas en República Checa, Rumanía y Polonia[55].

Por otra parte, en 2024 un ciberataque afectó a la empresa danesa de aguas, lo que permitió la manipulación externa de la presión de las bombas y provocó la rotura de diversas tuberías de la red. Además, durante los comicios locales de ese mismo año se produjeron ciberataques DDoS contra los sistemas informáticos institucionales. En ambos casos, la inteligencia danesa acusó a grupos vinculados al Kremlin —Z-Pentest y NoName057(16)— de ser los responsables[56].

[53] EUVSDISINFO. «Las mentiras de la Plaza Roja: propaganda en el desfile, en Internet y en las calles».
[54] HAECK, P. «TikTok removed 3 influence campaigns during Romania's elections – European Parliament», *Politico*. 3 de diciembre de 2024. Disponible en: https://www.politico.eu/article/tiktok-removed-3-influence-campaigns-during-romania-elections-european-parliament/ (consultado 11/3/2026); REUTERS. «Kremlin denies interference in Romanian election», *Reuters*. 29 de noviembre de 2024. Disponible en: https://www.reuters.com/world/europe/kremlin-denies-russian-interference-romanian-election-2024-11-29/ (consultado 11/3/2026).
[55] AFP. «Lituania acusa a seis extranjeros de terrorismo por atacar ayuda destinada a Ucrania», *La Nación*. 16 de enero de 2026. Disponible en: https://www.lanacion.com.ar/agencias/lituania-acusa-a-seis-extranjeros-de-terrorismo-por-atacar-ayuda-destinada-a-ucrania-nid16012026/ (consultado 11/3/2026);
[56] BRYANT, M. «Denmark says Russia behind cyber-attacks», *The Guardian*. 18 de diciembre de 2025. Disponible en: https://www.theguardian.com/world/2025/dec/18/denmark-says-russia-was-behind-two-destructive-and-disruptive-cyber-attacks (consultado 11/3/2026).

El Gobierno alemán ha acusado recientemente a Moscú de ser el responsable de una serie de acciones híbridas hostiles desarrolladas entre 2024 y 2025, cuyo objetivo habrían sido tanto los sistemas de gestión del tráfico aéreo como las elecciones federales alemanas. Las acciones habrían sido llevadas a cabo por el grupo APT28, mencionado anteriormente[57].

Especialmente preocupantes han sido las violaciones del espacio aéreo de los países miembros de la OTAN por parte de drones rusos. En julio, Lituania informó de que dos drones rusos, en distintas fechas, se habían adentrado en su territorio, probablemente por un error técnico que los alejó de su objetivo en Ucrania. El 8 de septiembre, un dron ruso violó el espacio aéreo rumano para atacar Ucrania. El 9 de septiembre, al menos 19 drones rusos sobrevolaron el espacio aéreo polaco. El número de vehículos no tripulados hace dudar de la hipótesis de un fallo técnico y apunta la posibilidad de que se tratara de una acción en la zona gris. El 13 de septiembre se derribó un dron ruso en Rumanía. Dos días después, el 15 de septiembre, otro dron aéreo fue derribado en Varsovia. Estas incursiones impulsaron al Gobierno polaco a invocar el artículo 4 del Tratado de la OTAN, un mecanismo raramente utilizado que se activa cuando un miembro se ve amenazado y que da lugar a un debate formal en el seno de la Alianza[58].

En paralelo a los incidentes anteriormente mencionados, diversos países de la OTAN denunciaron a finales de septiembre la presencia de drones no identificados cerca de bases militares y de aeropuertos civiles, lo que perturbó gravemente el tráfico aéreo. Así, Dinamarca vio afectadas las operaciones de los aeropuertos de Copenhague, Aalborg, Billund, Esbjerg y Sønderborg. Días después, se vio afectado el aeropuerto noruego de Oslo. Otros incidentes se han denunciado en Francia y Alemania, sin que quedara claro el origen ni la finalidad de los drones aéreos, que eran de tamaño reducido[59].

El acoso a la infraestructura aérea de los países miembros de la OTAN se complementa con constantes interferencias en el GPS —sistema de posicionamiento global—. La

[57] ISSEL, S. «Alemania acusa a Rusia de ciberataque al control aéreo», *Euronews*. 12 de diciembre de 2025. Disponible en: https://es.euronews.com/2025/12/12/alemania-acusa-rusia-ciberataque-control-aereo-desinformacion-electora

[58] SCHWIRTZ, M. y QASIM, N. «La OTAN dice que utilizó aviones de combate para derribar drones rusos sobre Polonia», *The New York Times*. 10 de septiembre de 2025. Disponible en: https://www.nytimes.com/es/2025/09/10/espanol/mundo/polonia-rusia-drones-ucrania.html (consultado 11/3/2026).

[59] DESMARAIS, A. «Del Báltico al Mediterráneo: la incursión de drones en países europeos pone en alerta a la defensa», *Euronews*. 30 de septiembre de 2025. Disponible en: https://es.euronews.com/next/2025/09/30/del-baltico-al-mediterraneo-la-incursion-de-drones-en-paises-europeos-pone-en-alerta-a-la- (consultado 11/3/2026).

afectación, en agosto de 2025, del vuelo chárter en el que viajaba la Comisión Europea de Polonia a Bélgica visibilizó una estrategia que ha afectado a miles de aeronaves durante los últimos años, especialmente a aquellas que transitan por países fronterizos con Rusia o por el enclave ruso de Kaliningrado[60].

También son destacables diversos incidentes producidos en el mar Báltico que dieron lugar al corte de cables submarinos vitales para diversas infraestructuras regionales. Así, en noviembre de 2024, los cables de telecomunicaciones BCS East-West Intelink y C- Lion1, que unen Lituania-Suecia y Alemania-Finlandia respectivamente, fueron dañados, y se sospechó de un barco chino que había partido de un puerto ruso[61]. Poco después, en diciembre de 2024, el cable eléctrico Estlink-2 y cuatro cables de telecomunicaciones que conectan Finlandia y Estonia fueron cortados o dañados por el petrolero Eagle S, con bandera de las Islas Cook, pero vinculado a la «flota fantasma» que Rusia emplea para evadir las sanciones internacionales. Las autoridades filandesas abordaron el buque y presentaron cargos contra los oficiales por daño criminal agravado e interferencia de comunicaciones[62]. Finalmente, el 31 de diciembre de 2025, el cable submarino de telecomunicaciones Elisa, que conecta Finlandia con Estonia, fue dañado por el carguero Fitburg, con bandera de San Vicente y las Granadinas, que había partido del puerto ruso de San Petersburgo. Las autoridades finlandesas abordaron el barco e iniciaron una investigación por daño criminal agravado e interferencia de telecomunicaciones[63] (Pohjanpalo, 31 de diciembre de 2025).

En síntesis, en el presente apartado se ha expuesto una selección no exhaustiva de hechos atribuidos —o susceptibles de atribuirse— a la Federación Rusa que, de forma directa o indirecta, han afectado a la seguridad nacional y colectiva de los países miembros de la OTAN. Las acciones presentadas pueden organizarse en la siguiente tabla tipológica:

[60] AYUSO, S. «El avión en el que viajaba Von der Leyen sufre interferencias rusas en el GPS», *El País*. 1 de septiembre de 2025. Disponible en: https://elpais.com/internacional/2025-09-01/el-avion-en-el-que-viajaba-von-der-leyen-sufre-interferencias-rusas-en-el-gps.html (consultado 11/3/2026).
[61] ASTIER, H. y KIRBY, P. «Undersea cables severed in Baltic Sea raise security concerns», *BBC*. 19 de noviembre de 2024. Disponible en: https://www.bbc.com/news/articles/c9dl4vxw501o (consultado 11/3/2026).
[62] LEHTO, E. y SYTAS, A. «Finland boards oil tanker suspected of causing internet, power cable outages», *Reuters*. 26 de diciembre de 2024. Disponible en: https://www.reuters.com/world/europe/finland-police-investigate-role-foreign-ship-after-power-cable-outage-2024-12-26/ (consultado 11/3/2026).
[63] POHJANPALO, K. «Finlandia toma un buque por causar daños a cable submarino de telecomunicaciones», *El Financiero*. 31 de diciembre de 2025. Disponible en: https://www.elfinanciero.com.mx/mundo/2025/12/31/finlandia-toma-un-buque-por-causar-danos-a-cable-submarino-de-telecomunicaciones/ (consultado 11/3/2026).

Tipología de actividades híbridas desarrolladas por Rusia en Ucrania y en la zona gris de la OTAN			
N.º	**Tipo de actividades**	**Descripción**	**Objetivo**
1	Ciberataques	Ataques a infraestructuras críticas, DDoS, *hack and leak*.	Degradación, señalización y coste reputacional y material.
2	Desinformación / Influencia	Campañas sostenidas, bots, manipulación de plataformas y medios de comunicación y sociales.	Polarización política y social, erosión de confianza en las instituciones.
3	Captación y coerción política	Apoyo a partidos y redes prorrusas, compra de influencia.	Modificar preferencias y políticas internas.
4	Sabotaje de infraestructuras críticas	Incendios, explosiones, corte de cables submarinos.	Coste económico y demostrar vulnerabilidad.
5	Presión militar no atribuible o con escaso coste	Drones, violaciones de espacio aéreo, interferencias GPS.	Delimitación de umbrales y cálculo de riesgos.
6	Uso de proxies	Actores interpuestos, negación plausible.	Evitar activación de mecanismos de defensa.

Tabla 1. Tipología de actividades híbridas desarrolladas por Rusia en Ucrania y en la zona gris de la OTAN. Elaboración propia.

Esta tipología muestra que la lógica común no es la obtención de una victoria inmediata, sino la generación de fricción acumulada sobre tres variables críticas de la disuasión —capacidad, determinación y comunicación—, lo que deteriora gradualmente la credibilidad aliada sin cruzar el umbral del conflicto armado. El recurso sistemático por parte de Moscú a este tipo de acciones evidencia la existencia de una confrontación entre Rusia y la OTAN, que, afortunadamente, aún no ha alcanzado el umbral de intensidad propio de un conflicto armado internacional.

Las estrategias e instrumentos desarrollados por Rusia en la zona gris de la confrontación, ya sea que busquen obtener réditos geopolíticos sin recurrir a la guerra o preparar el escenario para el inicio de un conflicto armado localizado, son, y esto es un hecho, una amenaza para la seguridad nacional de los países limítrofes, para la seguridad colectiva de la OTAN y para los principios del Derecho Internacional sobre los que se asienta el sistema de naciones surgido tras la Segunda Guerra Mundial. Así, los países miembros de la OTAN han de tomar conciencia de la situación y actuar en consecuencia.

La disuasión: un elemento clave para la prevención del conflicto armado

Más allá de su diversidad, los hechos expuestos anteriormente responden a una misma lógica: erosionar de forma gradual y sistemática las condiciones de disuasión existentes. Por ello, es pertinente analizar los efectos que estos han producido sobre la Alianza y qué instrumentos permiten negar beneficios o imponer costes sin provocar una escalada armada.

Hasta el momento, la respuesta de la OTAN no ha sido unánime ni adecuada. Respecto a lo primero, Hungría con Orbán, Turquía con Erdoğan y Estados Unidos con Trump han sido continuamente reticentes —o contradictorios— con determinados compromisos, incluso con el que implica el artículo 5 del Tratado del Atlántico Norte, referido al principio de defensa colectiva. En referencia a lo segundo, desde el inicio de la agresión rusa contra Ucrania la OTAN activó sus planes de defensa, con el despliegue de fuerzas terrestres, aéreas y marítimas en el este de Europa. Se emplearon elementos de alta preparación de la Fuerza de Respuesta de la OTAN, colocando a más de 40.000

efectivos bajo mando directo aliado, apoyados por despliegues nacionales adicionales. Además, en marzo de 2022, la Alianza acordó crear cuatro nuevos grupos de combate multinacionales en Bulgaria, Hungría, Rumanía y Eslovaquia, que se sumaron a los ya existentes en Estonia, Letonia, Lituania y Polonia[64]. Sin embargo, estas medidas, aunque limitadas, tienen un carácter preventivo para un escenario de conflicto armado convencional, pero no constituyen un instrumento adecuado para hacer frente a una confrontación en la zona gris.

Así, por ejemplo, derribar los baratos drones rusos que incursionan en el espacio aéreo de la OTAN con carísimos misiles aire-aire, disparados desde costosos aviones de combate F-35 o Eurofighter Typhoon, no es algo sostenible ni adecuado. Frente a ello, los autores coinciden en que los países miembros de la OTAN deben realizar esfuerzos significativos por restaurar un instrumento fundamental en la prevención de los conflictos armados: la disuasión.

Según Jordán[65]: «La disuasión es una variable relacional, resultado de una interacción en la que el disuadido opta por no llevar a cabo una acción —que de otro modo sí realizaría— al estimar los costes que puede entrañar». Así, el objetivo del actor que ejercería la disuasión —la OTAN— es influir en el cálculo de riesgos y beneficios de la otra parte —Rusia— para disuadirla de llevar a cabo una determinada acción. La disuasión puede ejercerse mediante negación —dificultando la acción o minimizando las ganancias— o mediante represalia —maximizando los costes mediante castigo—, y puede recurrirse a una amplia serie de instrumentos: amenazas militares, diplomacia, economía, información, sanciones, etcétera[66].

Si los actores llegan a la conclusión de que los beneficios de atacar primero no merecen los costes que habría que asumir, se alcanza una estabilidad estratégica que aleja la posibilidad de un conflicto armado[67]. A este principio habría que sumar la inclusión de garantías, ya que, si bien «la disuasión se basa en amenazas asociadas a traspasar

[64] NATO. *Strategic Concept 2022*, pp. 15-16.

[65] JORDÁN, J. «La disuasión en la zona gris: una exploración teórica», *Revista Española de Ciencia Política*, n.º 59. 2022, pp. 65-88.

[66] FREEDMAN, L. «Deterrence», *Polity Press*. 2004; JORDÁN, J. «La disuasión en la zona gris: una exploración teórica», *Revista Española de Ciencia Política*, n.º 59. 2022, pp. 65-88; KNOPF, J. W. «The fourth wave in deterrence research», *Contemporary Security Policy*, vol. 31, n.º 1. 2010, pp. 1-33. Disponible en: https://doi.org/10.1080/13523261003640819 (consultado 11/3/2026); SNYDER, G. H. *Deterrence and Defense: Toward a Theory of National Security*. Princeton University Press, 1961.

[67] BRODIE, B. «Strategy in the Missile Age», *RAND Corporation*. 1959; JORDÁN, J. «La disuasión en la zona gris: una exploración teórica», *Revista Española de Ciencia Política*, n.º 59. 2022, pp. 65-88.

determinados límites», también debe «aliviar la inseguridad de la otra parte garantizando que no tiene nada que temer si los respeta»[68], con el fin de evitar caer en las perniciosas dinámicas del dilema de la seguridad. Por último, particularmente en el caso referido a Rusia, es relevante un concepto desarrollado en las dos últimas décadas: la disuasión a medida, lo que implica «conocer en profundidad los valores, normas, intereses y condicionantes de quienes toman las decisiones para comprender su mentalidad o cultura estratégica»[69], lo que obliga a ampliar desde una perspectiva disciplinar el análisis del actor. Gran parte de la literatura académica referida a la disuasión proviene de la Guerra Fría y está pensada desde una óptica convencional y bipolar.

Su aplicación en una confrontación que se desarrolla en la zona gris no está exenta de problemas, especialmente frente a aquellas acciones que conllevan pocos riesgos para el agresor —por ejemplo, ataques cibernéticos—, que son difíciles de impedir —negación— y complejas de represaliar por temor a provocar una escalada hacia el conflicto armado[70]. Así, Jordán advierte de dos grandes problemas para una disuasión efectiva en la zona gris. El primero es que es «dudosamente efectiva» en los umbrales de intensidad bajos, mientras que tiene «mayores probabilidades de éxito» en los altos. El segundo, que, en la zona gris, caracterizada por ser un área volátil, incierta, compleja y ambigua, es tremendamente difícil controlar la escalada de la confrontación[71].

Sumados a los anteriores, los autores quieren destacar un tercero: la ausencia de un cuerpo legal suficiente que regule una confrontación en la zona gris. Al no alcanzar la categoría de conflicto armado, ni el Derecho Internacional a la legítima defensa —*ius ad bellum*— ni el Derecho Internacional Humanitario —*ius in bello*— resultan aplicables a la cuestión, por lo que las acciones en este escenario deben guiarse únicamente por el Derecho Internacional de los Derechos Humanos. Esto, en el caso que se refiere a Rusia y a la OTAN, genera una «asimetría legal», ya que los gobiernos occidentales son más dependientes de la crítica de la opinión pública ante sus acciones y ello limita sus capacidades de respuesta[72]. Así, parece que Rusia, por sus características geopolíticas, posee una ventaja significativa frente a la OTAN en la confrontación que se desarrolla

[68] JORDÁN**.** «La disuasión en la zona gris: una exploración teórica», p. 71.
[69] Ibíd.
[70] Ibíd.
[71] Ibíd., p. 77.
[72] SOTO SILVA. «La zona gris, un desafío para la conducción política y estratégica», p. 13.

en la zona gris. No obstante, de los países miembros de la OTAN y de sus sociedades depende que esta ventaja sea circunstancial y no estructural. A diferencia de la disuasión clásica, centrada en evitar el inicio de un conflicto armado, la disuasión en la zona gris busca modular comportamientos, establecer límites tácitos y gestionar la escalada dentro de un entorno de competencia permanente.

Una disuasión efectiva se fundamenta en la credibilidad, «entendida como la probabilidad percibida de que el disuasor materialice su amenaza al darse las condiciones que supuestamente deberían activar la disuasión»[73]. Esta depende de tres factores: capacidad —recursos materiales para defenderse o represaliar—, determinación —voluntad política para emplear las capacidades— y comunicación —eficaz para que resulte creíble—.

Es de destacar que estos tres factores no suman entre sí, sino que se multiplican[74]. Por lo tanto, valores bajos en uno de ellos lastran la eficacia de la disuasión. Según Jordán[75], una estrategia de disuasión efectiva debe ser «no escalatoria, a la medida y con garantías, contar con credibilidad basada en capacidades, determinación y comunicación adaptadas a la zona gris, y asumir que se trata de una disuasión acumulativa». Respecto a esto último, Jordán afirma que la disuasión en la zona gris es «resultado de múltiples interacciones inamistosas en las que el disuasor es capaz de imponerse y transmitir la necesidad de respetar determinados límites. La disuasión acumulativa asume *de facto* el fracaso repetido tanto de la disuasión general como de la disuasión inmediata. Sin embargo, trata de alcanzar la estabilidad estratégica a través de un proceso de aprendizaje en el que van tomando forma normas de conducta, a veces conocidas como reglas del juego»[76].

Desde la perspectiva de la OTAN, y con base en los propósitos y principios del *Strategic Concept 2022*, la disuasión por negación ha de basarse en la resiliencia, la disuasión integrada y un enfoque que implique a toda la sociedad. La experiencia de Ucrania ha demostrado la importancia de este enfoque, ya que la resistencia del pueblo ucraniano «se vertebra a partir de una combinación de numerosas formas y prácticas de resiliencia como característica social de autosuficiencia, autonomía y autoorganización […]. Se trata

[73] JORDÁN**.** «La disuasión en la zona gris: una exploración teórica», p. 69.
[74] Ibíd., p. 69.
[75] Ibíd., pp. 78-82.
[76] Ibíd., p. 82.

de una resiliencia híbrida que se basa en una forma de gobernanza descentralizada, en la sostenibilidad de las redes sociales, en una política informativa fiable y en una firme adhesión pública a la idea de una guerra justa. […] La resiliencia híbrida constituye el punto esencial de la supervivencia de Ucrania como nación»[77]. Así, la disuasión por negación de la OTAN ha de pretender incrementar la resiliencia aliada para, mediante estrategias de prevención estructural, la reducción de vulnerabilidades y la denegación de ventajas estratégicas, negar beneficios estratégicos a actores hostiles. Por otra parte, y también alineada con el *Strategic Concept 2022*, la disuasión por represalia de los países miembros de la OTAN ha de fundamentarse, más allá de los instrumentos militares convencionales, en la imposición de costes coordinados y proporcionales mediante sanciones multisectoriales, atribución pública, respuestas coordinadas, costes reputacionales, así como medidas legales y diplomáticas.

Para ejemplificar las pretensiones anteriores, y sin buscar exhaustividad, sino ofrecer una aproximación a los posibles mecanismos de disuasión por negación y por represalia frente a actividades híbridas en el entorno de competencia estratégica de la zona gris, se expone una tabla elaborada a partir de la literatura académica de autores diversos como Jordán[78], Mearsheimer[79], Kofman y Rojansky[80], Renz y Smith[81], Hoffman[82], Mazarr[83] o Nye[84]. Alineados con el *Strategic Concept 2022*, los mecanismos de disuasión frente a actividades híbridas se basan en una combinación de resiliencia, prevención y la imposición de costes coordinados, con el objetivo de reforzar la capacidad de los aliados para negar beneficios estratégicos a los actores hostiles y responder de manera proporcionada y legal, evitando la escalada armada y preservando la estabilidad estratégica en un contexto de competencia sistémica.

Con ella se pretende combinar un marco neorrealista con un mapeo sistemático de las actividades híbridas más recurrentes y su traslación a mecanismos de disuasión

[77] KURNYSHOVA, Y. y MAKARYCHEV, A. «La guerra de Rusia y la sociedad ucraniana», en *Amenazas híbridas, orden vulnerable*. CIDOB Report, n.º 8, CIDOB, 2022, pp. 47-54.
[78] JORDÁN, J. «La disuasión en la zona gris: una exploración teórica», *Revista Española de Ciencia Política*, n.º 59. 2022, pp. 65-88; JORDÁN, J. «El conflicto internacional en la zona gris», *Revista Española de Ciencia Política*, n.º 48. 2018, pp. 129-151. Disponible en: https://doi.org/10.21308/recp.48.05.
[79] MEARSHEIMER, J. J. *The Tragedy of Great Power Politics*. W. W. Norton, 2001.
[80] KURNYSHOVA y MAKARYCHEV. «La guerra de Rusia y la sociedad ucraniana».
[81] RENZ, B. y SMITH, H. *Russia and Hybrid Warfare – Going Beyond the Label*. Aleksanteri Papers, 2016.
[82] HOFFMAN, F. G. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, 2007.
[83] MAZARR, M. J. *Mastering the Gray Zone*. RAND Corporation, 2015.
[84] NYE, J. S. *The Future of Power*. PublicAffairs, 2011.

aplicables en la zona gris y alineados con el *Strategic Concept 2022* de la OTAN. Actividades híbridas en el entorno de la competencia estratégica de la zona gris y posibles mecanismos de disuasión por negación y por represalia.

Actividades híbridas en el entorno de la competencia estratégica de la zona gris y posibles mecanismos de disuasión por negación y por represalia			
N.º	**Actividades híbridas**	**Mecanismos de disuasión por negación**	**Mecanismos de disuasión por represalia**
1	Ciberoperaciones contra infraestructuras críticas	Resiliencia cibernética aliada, redundancia de sistemas	Atribución pública y sanciones
2	Ataques DDoS a instituciones públicas	Infraestructura digital resiliente	Contramedidas legales y sanciones
3	Operaciones de robo y difusión de información (*hack and leak*)	Protección de datos y ciberhigiene	Procesos judiciales y sanciones
4	Interferencia en procesos electorales	Protección electoral y comunicación estratégica (*StratCom*)	Sanciones y restricciones políticas
5	Desinformación estratégica sostenida	Alfabetización mediática y detección temprana	Restricciones a medios estatales
6	Saturación informativa deliberada (*information flooding*)	Capacidades de verificación y comunicación institucional	Atribución coordinada
7	Manipulación algorítmica en redes sociales	Regulación de plataformas	Multas y bloqueos regulatorios
8	Uso de IA generativa para operaciones cognitivas	Gobernanza de IA y detección técnica	Sanciones tecnológicas
9	Apoyo encubierto a partidos o movimientos políticos	Transparencia financiera	Sanciones individuales
10	Instrumentalización de minorías étnicas	Protección de derechos e inclusión social	Misiones de la OSCE y sanciones

11	Presión transnacional sobre diásporas	Protección policial y consular	Sanciones personales
12	Narrativas históricas revisionistas	Diplomacia pública y educación estratégica	Condenas multilaterales
13	Amenazas nucleares retóricas	Comunicación estratégica aliada	Aislamiento diplomático
14	Incursiones aéreas provocativas	Vigilancia integrada y medios adecuados de negación	Protestas diplomáticas y sanciones
15	Incursiones marítimas ambiguas	Conciencia situacional marítima	Sanciones y no reconocimiento
16	Sabotaje encubierto de cables submarinos	Monitoreo y redundancia	Atribución y sanciones
17	Interferencia en sistemas globales de navegación por satélite	Sistemas alternativos y protección	Medidas diplomáticas
18	Uso de fuerzas irregulares sin identificación	Control administrativo del territorio	No reconocimiento jurídico
19	Apoyo encubierto a proxies armados	Cooperación policial y fronteriza	Designación y sanciones
20	Militarización encubierta de espacios civiles	Inspecciones legales	Sanciones multilaterales
21	Coerción energética selectiva	Diversificación energética	Sanciones sectoriales
22	Dependencia inducida de recursos críticos	Diversificación y reservas	Medidas comerciales defensivas
23	Coerción económica selectiva	Apoyo estatal y diversificación	Sanciones económicas
24	*Dumping* estratégico en sectores clave	Defensa comercial legal	Aranceles compensatorios
25	Interferencia en cadenas de suministro	Control de dependencias estratégicas	Medidas defensivas para eliminar la interferencia
26	Uso de empresas privadas como instrumentos estatales	Control de inversiones	Congelación de activos
27	Adquisiciones hostiles fragmentadas	Evaluación y supervisión de inversiones	Bloqueo legal

28	Espionaje económico y tecnológico	Protección de I+D+I	Expulsiones y sanciones
29	Desestabilización financiera encubierta	Supervisión macroprudencial	Medidas regulatorias
30	Presión sobre mercados de seguros y *rating*	Regulación financiera	Respuestas coordinadas
31	*Lawfare* estratégico	Capacidades jurídicas especializadas	Litigio internacional
32	Bloqueo deliberado de organizaciones internacionales	Coordinación multilateral	Aislamiento político
33	Captura normativa en organismos técnicos	Presencia institucional activa	Impugnación multilateral
34	Dilación estratégica en mecanismos legales	Reforma procedimental	Presión diplomática
35	Uso de las ONG u organizaciones pantalla	Control de financiación	Cancelación legal
36	Instrumentalización de crisis migratorias	Gestión fronteriza cooperativa	Sanciones diplomáticas y económicas
37	Uso estratégico de visados y movilidad	Coordinación consular	Medidas de reciprocidad
38	Instrumentalización del turismo	Diversificación económica	Restricciones selectivas
39	Normalización gradual de hechos consumados ilegales	Presencia institucional constante	Política de no reconocimiento
40	Erosión sistemática de confianza en instituciones democráticas	Resiliencia integral de la sociedad	Imposición prolongada de costes

Tabla 2. Actividades híbridas en el entorno de competencia estratégica de la zona gris y posibles mecanismos de disuasión por negación y por represalia. Elaboración propia.

En referencia a la tabla, conviene destacar que los mecanismos de disuasión por negación recogidos en la tabla se alinean con el enfoque de la OTAN de fortalecimiento de la resiliencia, con el objetivo de reducir las vulnerabilidades políticas, económicas, sociales y tecnológicas que los actores hostiles explotan mediante actividades híbridas.

Además, los mecanismos de disuasión por represalia señalados no implican el uso de la fuerza armada, sino la imposición de costes políticos, económicos, jurídicos y reputacionales de manera coordinada entre los aliados. Así, tanto los mecanismos de negación como los de represalia están situados deliberadamente por debajo del umbral que activaría el artículo 5, pero dentro del artículo 4 en el que «las Partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes fuese amenazada»[85], lo que favorece respuestas coordinadas.

Así, frente a las acciones rusas en la zona gris y pese a los desafíos que estas suponen, es posible oponer mecanismos adecuados de disuasión por negación o represalia. Sin embargo, la gran cuestión es si los países miembros de la OTAN articularán colectivamente capacidad, determinación y comunicación para construir una disuasión verdaderamente creíble.

Conclusiones

El análisis desarrollado a lo largo de este trabajo pone de manifiesto que la relación entre Rusia y la OTAN no puede ser comprendida adecuadamente si se limita a una lectura binaria y dicotómica entre guerra y paz. Desde hace más de dos décadas, el Kremlin ha venido desplegando una estrategia sostenida de competencia estratégica por debajo del umbral del conflicto armado internacional, primero en su denominado «extranjero próximo» y, de forma creciente, contra los países miembros de la OTAN. Esta dinámica, que se inscribe plenamente en lo que la literatura especializada ha conceptualizado como la zona gris, constituye hoy una amenaza directa para la seguridad nacional de los Estados miembros y para la seguridad colectiva de la organización atlántica.

Desde una perspectiva neorrealista, el comportamiento ruso responde a una lógica de búsqueda de seguridad y de revisión del *statu quo* internacional en un sistema anárquico, competitivo y en transformación. Sin embargo, el recurso sistemático a instrumentos híbridos no solo erosiona los principios del Derecho Internacional y las normas que sustentan el orden internacional, sino que incrementa los riesgos de una escalada no

[85] NATO. *North Atlantic Treaty*, 1949. Disponible en: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty (consultado 11/3/2026).

deseada y de error de cálculo. Lejos de constituir acciones aisladas u oportunistas, estos instrumentos forman parte de una estrategia coherente y acumulativa destinada a debilitar la cohesión aliada, explotar vulnerabilidades estructurales y condicionar la toma de decisiones políticas.

Desde la perspectiva de Waltz, el Estado debe garantizarse el poder suficiente para su supervivencia y, con ello, optar por la acción que sea necesaria para lograrlo. Esto es lo que Rusia ha estado llevando a cabo desde el inicio de la guerra en Ucrania. Sin duda, los nuevos instrumentos utilizados en la guerra híbrida, como el uso de drones, han cambiado el curso del conflicto desde sus inicios, al igual que los diversos ciberataques, que cada vez son más sofisticados. Por lo tanto, se ha vuelto aún más complicado garantizar la seguridad de los civiles y de los militares, tanto en Ucrania como en la Federación Rusa. Estas amenazas causan daños que provocan desde pérdidas económicas de miles de dólares hasta múltiples bajas humanas. Es crucial comprender que, en este tipo de guerra, se puede emplear cualquier forma de poder que el Estado tenga a su alcance —económico, militar, diplomático, social o cibernético—. Desde la perspectiva rusa, garantizar la seguridad nacional implica proteger su esfera de influencia a toda costa, utilizando todas las capacidades a su alcance. Así, la denominada zona gris se caracteriza por ser un espacio particularmente volátil.

El estudio empírico de los casos expuestos evidencia que muchos de los patrones de comportamiento desplegados por Rusia frente a Ucrania antes de 2022 se han reproducido, con las adaptaciones necesarias, en el entorno de la OTAN. La diferencia fundamental reside en que, mientras Ucrania fue progresivamente aislada y erosionada hasta el inicio del conflicto armado, los países aliados cuentan con mecanismos de cooperación, capacidades colectivas y marcos institucionales que, si se emplean de manera coherente y coordinada, pueden impedir que la confrontación en la zona gris derive en una guerra convencional de mayor alcance. No obstante, esta potencialidad no se traduce automáticamente en una disuasión efectiva.

El trabajo ha mostrado que los mecanismos tradicionales de disuasión, concebidos para prevenir conflictos armados, resultan insuficientes para responder a una confrontación caracterizada por la ambigüedad, la fragmentación y la acumulación progresiva de acciones hostiles. La disuasión en la zona gris exige un enfoque adaptado, basado en la combinación de la disuasión por negación y por represalia, la construcción de resiliencia

social, la coordinación interinstitucional y la imposición de costes proporcionales, creíbles y sostenidos en el tiempo. Se trata de modular comportamientos, establecer límites tácitos y gestionar la escalada dentro de un entorno de competencia permanente.

Es crucial que los países miembros de la OTAN y su ciudadanía asuman que la defensa del Estado de derecho democrático y de la seguridad colectiva no se libra únicamente en el ámbito militar, sino también en los espacios político, informativo, económico, tecnológico y social. La credibilidad de la disuasión aliada dependerá, en última instancia, de la capacidad de articular de manera coherente, las capacidades, la determinación política y la comunicación estratégica clara y unificada.

En definitiva, la confrontación entre Rusia y la OTAN ya está en curso, aunque se desarrolle mayoritariamente en la zona gris. Ignorar esta realidad o subestimarla equivale a repetir errores lejanos y recientes, con consecuencias potencialmente más graves. La toma de conciencia que se reclama en este trabajo no persigue normalizar la confrontación ni abandonar los principios del orden internacional, sino reconocer las condiciones reales en las que hoy se estructura la competencia estratégica. Solo a partir de ese reconocimiento será posible diseñar políticas de disuasión eficaces que contribuyan, paradójicamente, a preservar la paz y evitar que la zona gris se transforme en un nuevo conflicto armado internacional en Europa.

*Antonio Gil Fons y Saraí Valerdi Macías**