ieee.es
Instituto Español de Estudios Estratégicos

Research
Paper

02/2026 22/04/2026

Antonio Gil Fons, Sarai Valerdi Macías[1]

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

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

NOTE:** The ideas contained in the ***Research Papers are the responsibility of the authors and do not necessarily reflect the views of the IEEE or the Ministry of Defence.

How to cite this document:

Gil Fons, Antonio., Valerdi Macias, Sarai. *The Russia–NATO Confrontation in the Gray Zone: Towards a Necessary Strategic Awareness*. IEEE Research Paper 00/2025. IEEE web link and/or bie link[3] (accessed day/month/year).

Antonio Gil Fons, Sarai Valerdi Macías

“He who desires peace, therefore, must prepare for war”. These words, written in the fourth century by the Roman Flavius Vegecius in his work *Epitoma rei militari*—often summarized as “if you want peace, prepare for war” —remain, in theas “ors' opinion, relevant today. The end of history proclaimed by Fukuyama seems to be behind us, and related dogmas appear to be being overcome. International order and law are being challenged by powerful actors, while mechanisms for multilateral cooperation and dialogue are proving inefficient or incapable. In a world that seems to be accumulating dangerous geopolitical dynamics, the United Nations Charter pales in comparison to the behavior, by action or omission, of its signatories.

Unfortunately, in the last decade, there have been several events that are shameful from a human, moral, ethical, and legal point of view. This calls for profound reflection, debate, consensus, and mechanisms to prevent their repetition and consequences. A clear example of the latter is the armed conflict between Russia and Ukraine. Although it officially began in February 2022 with the military invasion of Ukraine by Russian armed forces, an unconventional confrontation between Moscow and Kyiv had been brewing for the previous two decades. This confrontation, which fell below the threshold of international armed conflict regulated by international humanitarian law, was mainly characterized by Moscow's use of hybrid instruments against Ukraine in the so-called “gray zone.” Thus, for years, Ukraine was harassed with cyberattacks, sabotage, electoral interference, coercive diplomacy, economic pressure, massive disinformation campaigns, armed groups, and so on. This broad-spectrum hybrid strategy, developed over many years, helped create a situation favorable to what the Kremlin called the “special military operation” launched in 2022 against Ukraine.

The problem analyzed in this text is that the hybrid strategies and instruments that the Kremlin ordered to be implemented and perfected in Ukraine[2] over two decades are now being replicated against member countries of the North Atlantic Treaty Organization (NATO). In a series of increasingly daring actions, the gray zone between Russia and NATO has taken on new dynamics that could precede, as in the case of Ukraine, an international armed conflict with conventional characteristics.

This paper seeks to answer the question of the extent to which the hybrid strategies deployed by Russia against Ukraine prior to 2022 are being replicated against NATO member countries, and what implications this has for allied deterrence. Faced with the threat of being dragged into a conflagration that would shatter what remains of peace on the old continent, the authors believe that NATO, while recognizing the internal political differences that condition its capacity for action, must prepare for conventional conflict, but also for confrontation in the gray zone, since effective deterrence in this area is a key element in preventing a new war. As Flavius Vegetius reminded us, if you want peace, you must prepare for war, including confrontation in the gray zone.

The facts presented here are not intended to be exhaustive or causally equivalent, but rather to illustrate recurring patterns and mechanisms. They are selected and presented based on their strategic relevance, so that the evidence serves an analytical hierarchy.

The work is methodologically based on a neo-realist theoretical framework and security studies, with the analysis of a selection of cases and episodes documented in open sources, specialized reports, and academic literature, with a qualitative approach.

The cases are chosen for their relevance in illustrating the gradual projection of Russian hybrid instruments into NATO space, to identify patterns of behavior and logic of confrontation in the gray zone. It should be acknowledged, however, that there is an analytical bias, as Euro-Atlantic sources predominate for reasons of availability, verifiability, and relevance. It is considered that this limitation does not invalidate the patterns identified, but caution and rational criticism are recommended.

The text is divided into three sections. The first is a theoretical-conceptual approach to certain aspects that must be considered regarding the functioning of the international

[2] In this work, hybrid strategy is understood as the general framework for action, while hybrid instruments constitute the specific means—political, economic, informational, cybernetic, or military—used for its execution.

political system. Thus, the neorealist theory of international relations—as the main, but not exclusive, approach—and the concepts of national security and gray zone enrich the analysis. The second section is a non-exhaustive compilation of the hybrid instruments that the Kremlin has been using against NATO member countries over the last two decades. These examples serve to highlight a reality: that of the confrontation between Russia and NATO beyond Ukraine.

The third section focuses on deterrence, delving into the complexities that arise when applying traditional concepts and mechanisms to the gray zone, yet which are essential for preventing new international armed conflicts in Eastern Europe.
Finally, the conclusions will close with a text that aims to invite reflection and awareness of the current geopolitical circumstances, seeking to overcome the limitations of how we would like the world to be and promote, first, thinking about how it really is. With this structure, this research seeks to provide a systematic analysis of Russia's use of hybrid instruments against NATO and its environment, as well as to propose, based on the evidence, deterrence mechanisms adapted to the gray zone.

1. Neorealism in international relations, national security, and the gray zone

Neorealism is one of the most developed theories within the ever-dynamic discipline of International Relations. Conceptualized in the late 1970s by American scholar Kenneth Waltz, it sought to overcome the limitations of realist theory by introducing the structural aspect of the functioning of the international system into the analysis[3]. In the new approach advocated by Waltz, the state continues to be the main actor in international relations, but power, the final goal in realist theory, is now a means to achieve the real objective: security[4]. For Waltz, “in crucial situations [...] the ultimate concern of states is not power, but security”[5]. Given this fact, we must analyze “international events from a systemic level, where the actions of the great powers—which are the units that interact

[3] DE ALBA, José, “Realismo estructural”, en SCHIAVON, Jorge A.; ORTEGA, Adrián S.; LÓPEZ-VALLEJO, Marcela y VELÁZQUEZ, Rafael (eds.), *Teorías de Relaciones Internacionales en el siglo XXI: Interpretaciones críticas desde México*, UABC; BUAP; UANL; UPAEP, 2014, pp. 227-249. UABC; BUAP; UANL; UPAEP, 2014.
[4] Ibíd., p. 227–249.
[5] WALTZ, Kenneth N., “The Origins of War in Neorealist Theory”, *Journal of Interdisciplinary History*, 18 (4), 1988, pp. 615-628.

within the structure—influence the rest of the states, dictating the order and balance of forces"[6]. In other words, it is advisable to study both the agents and the system, which limits and conditions the behavior of the former[7]

According to Waltz, the system has three fundamental characteristics. The first of these is anarchy as an organizing principle. By this, he means the absence of a supranational body that imposes rules of behavior on states or has superior coercive power—think of the limited capabilities of the United Nations or the unpunished violation of numerous Security Council resolutions. In the absence of such authority, states are responsible for their own security[8]. "Each state pursues its own interests [...] in the manner it deems best" and, in the absence of a conciliatory body with the capacity to resolve disputes or enforce compliance, "force is a means to an end"[9], as Russian President Putin must have thought in reference to his problems with Ukraine. This anarchy favors a competitive environment where the strongest prevail[10], and where any type of collaboration between units—whether alliance, cooperation, détente, or even peace—is due to the circumstances of the prevailing anarchic structure and the capabilities and interests of the states requiring or agreeing to it.

The second characteristic of the system is that it is composed of units with similar functions but different capacities, which has an impact on the international dynamics that states will develop and mostly on their structural position. "Those who maintain capabilities and power retain broad decision-making capacity in foreign policy"[11].

[6] DE ALBA, José, "Realismo estructural", p. 243.

[7] KEOHANE, Robert O., *Instituciones internacionales y poder estatal: Ensayos sobre teoría de las relaciones internacionales*, Grupo Editor Latinoamericano, Buenos Aires, 1989; DE ALBA, José, "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] 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, José, "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.

[9] WALTZ, Kenneth N., *Man, the State and War: A Theoretical Analysis*, Columbia University Press, New York, 1954.

[10] 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/

[11] DE ALBA, José, "Realismo estructural", pp. 231 – 232.

Finally, the third major feature is the degree of concentration or diffusion of power, which defines the polarity of the system: multipolar, bipolar, unipolar, unimultipolar, etc. The degree of concentration or diffusion of power is not unalterable over time, varying from one system to another and from one time period to another[12]. Power capacities constitute the variable element of the structure, whose changes generate modifications in the international dynamics of cooperation and rivalry[13].

In this scenario of anarchy and competition between actors, a paradox has arisen whereby a state—for example, Russia—seeking to strengthen its security (invasion of Ukraine) causes an increase in its insecurity. This is what Herz[14] called the security dilemma, where, although a state may interpret—or argue—that its quest for greater power is due to defensive and survival issues, its environment—NATO—may perceive that such actions respond to offensive ambitions.

"When a great power takes measures to increase its security, it conversely decreases the security of others—and changes the balance of power"[15]. Faced with this problem, Waltz advocates a defensive realist approach, whereby states should not seek to maximize their power, but rather maintain an adequate amount to ensure their survival and make rational decisions regarding their foreign policy— 'do it because it is necessary'[16]. In contrast, Mearsheimer expounds an offensive realism in which he argues that the state should take advantage of any opportunity to gain more power, with its maximization and the achievement of hegemony being the fundamental objectives of action— "do it because it can be done"[17]. However, these proposals respond more to the question of how the system should work rather than how it works. In any case, neo-realism argues that the final goal pursued by states is security.

[12] KEOHANE, Robert O., Instituciones internacionales y poder estatal.

[13] KEOHANE, Robert O., *Instituciones internacionales y poder estatal: Ensayos sobre teoría de las relaciones internacionales*, Grupo Editor Latinoamericano, Buenos Aires, 1989; DE ALBA, José, "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.

[14] HERZ, John H., *Political Realism and Political Idealism: A Study in Theories and Realities*, University of Chicago Press, Chicago, 1951.

[15] DE ALBA, José, "Realismo estructural", p. 234.

[16] 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.

[17] Ibíd., p. 53

Undoubtedly, national security is a key organizing concept in the articulation of national and international policies of many states around the world. However, as Sagastegui[18] rightly points out, it is “a concept that is difficult to conceive and define in doctrine. [...] It has very broad margins and is so dependent on volatile circumstances” that it is extremely complex to define. For Israeli General Tal[19], “the concept of national security is about safeguarding the existence of a nation and defending its vital interests. Existence is the basic objective of security.” For his part, Laswell defined national security as “an absence of coercion from outside”[20]. Meanwhile, Lustgarden and Leigh assert that it is “the defense of democratic practice free from foreign manipulation, together with the ability to defend the independence of the nation and its territory against military attack”[21].

With the end of the Cold War, some academics — Buzan[22] —went beyond the traditional state-centric view and advocated "a broader vision, aimed at preserving the security of multiple stakeholders, such as vulnerable people, ethnic groups, and governments, among others," seeking to incorporate other types of threats into the concept, such as climate change, food insecurity, environmental degradation, resource depletion, etc[23]. An example of this expansionist vision can be found in Spain, which in Article 3 of the National Security Law defines it as “the action of the State aimed at protecting the freedom, rights, and well-being of citizens, guaranteeing the defense of Spain and its constitutional principles and values, as well as contributing, together with our partners and allies, to international security in fulfillment of the commitments assumed”[24].

From the study of a significant number of definitions, whether traditional or expansionist, three conclusions can be drawn: 1) it is the state that guarantees national security by safeguarding national sovereignty, territory, and the rights of its citizens, whether against

[18] SAGASTEGUI, F. Y., *La seguridad nacional en el Estado constitucional de derecho*, tesis doctoral, Universidad Carlos III de Madrid, Madrid, 2015.
[19] TAL, I. *National Security: The Israeli Experience*, Praeger Publishers, Westport, 2000.
[20] SAGASTEGUI, F. Y., La seguridad nacional en el Estado constitucional de derecho, p. 18.
[21] Ibíd., pp. 17 -18
[22] BUZAN, Barry, *Introducción a los estudios estratégicos: Tecnología militar y relaciones internacionales*, Ediciones Ejército, Madrid, 1991.
[23]SAGASTEGUI, F. Y., *La seguridad nacional en el Estado constitucional de derecho*, p. 20
[24] ESPAÑA, *Ley 36/2015, de 28 de septiembre, de Seguridad Nacional*, *Boletín Oficial del Estado*, núm. 233, 29 de septiembre de 2015, disponible en https://www.boe.es/eli/es/l/2015/09/28/36

internal or external threats; 2) the concept of national security has evolved—and continues to do so—over time; and 3) definitions of national security, threats, or vital interests are unique to each country and society, being the result of historical, sociological, political, and other factors[25].

The primary objective of national security must be to safeguard the existence of the nation-state, since, at least in liberal democratic regimes, it is a key and fundamental element in guaranteeing the enjoyment of rights by citizens. Based on this, the greatest threat to the existence of a nation-state usually stems from the existence of armed conflict, whether international or non-international in nature. It would be logical to think that, in contrast, peace represents an ideal situation for national security. However, formal peace does not necessarily imply the absence of confrontation, as there are a number of nuances that make up what has been described as a volatile area — "frequent, rapid, and significant changes" — uncertain —"events and outcomes are unpredictable"— complex—"multitude of issues and factors, some of which may be intricately interconnected"—and ambiguous—"diffuse environment" and it is difficult to know the real situation —: the gray zone[26].

Although this concept has a long history, having been coined at the beginning of the Cold War by thinkers such as Kennan and strongly revived in the post-Cold War era, its definition remains unclear. It has usually been defined as a situation between war and peace[27]. However, Soto Silva[28] states that "an international conflict in the gray zone arises when [...] countries seeking to alter the status quo in their favor employ multidimensional and synchronized strategies to gradually undermine their adversary and achieve their objectives." Therefore, the gray zone should not be understood as a space between war and peace, but rather as a "useful mechanism for forcing the status quo" by some revisionist state actors in an environment of strategic competition below the

[25] SAGASTEGUI, F. Y., *La seguridad nacional en el Estado constitucional de derecho.*

[26] SOTO SILVA, José, "La zona gris, un desafío para la conducción política y estratégica", *Cuadernos de Trabajo del Centro de Investigaciones y Estudios Estratégicos (ANEPE)*, número 6, 2021.

[27] JORDÁN, Javier, "El conflicto internacional en la zona gris", *Revista Española de Ciencia Política*, nº 48, 2018, pp. 129-151, disponible en: https://doi.org/10.21308/recp.48.05; SOTO SILVA, José, "La zona gris, un desafío para la conducción política y estratégica", *Cuadernos de Trabajo del Centro de Investigaciones y Estudios Estratégicos (ANEPE)*, nº 6, 2021.

[28] SOTO SILVA, José, "La zona gris, un desafío para la conducción política y estratégica", p. 8.

threshold of armed conflict[29]. In this sense, this paper distances itself from approaches that understand the gray zone as a mere transitional situation between war and peace. Thus, the authors conceive it as a sustained mode of strategic competition that is deliberately developed below the threshold of armed conflict, a conception that serves as an analytical framework for interpreting the Russia-NATO relationship over the last two decades.

The strategies and tactics developed in the gray zone are characterized by the multidimensionality and hybrid nature of the hostile methods they employ—disinformation, cyberterrorism, sabotage, support for irregular non-state forces, accumulation of small faits accomplis, coercive diplomacy, military deterrence, etc. They never reach the point of direct armed confrontation—thus remaining within the bounds of international law—due to the generation of asymmetric actions against conventional defenses (violation of airspace by drones), ambiguity that allows for plausible deniability or non-attribution (use of proxies), and the difficulty of quantifying their risks based on traditional models. This ambiguity makes it difficult to adopt clear and coherent responses, in many cases favoring a gradual escalation of confrontatio —actions to shape the environment, interference, destabilization, limited and selective use of force —[30]

Thus, the use of actions such as political subversion, economic coercion, operations to influence public opinion, faits accomplis, or claims of various kinds against other states, “keeping one's own society as a battlefield”[31], can achieve geopolitical objectives “that would be difficult to achieve through good-faith political and legal practice, but without

[29] Ibíd., p.10

[30] 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*, nº 48, 2018, pp. 129-151, disponible en https://doi.org/10.21308/recp.48.05; JORDÁN, Javier, “La disuasión en la zona gris: una exploración teórica”, *Revista Española de Ciencia Política*, nº 59, 2022, pp. 65-88; 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; SOTO SILVA, José, “La zona gris, un desafío para la conducción política y estratégica”, *Cuadernos de Trabajo del Centro de Investigaciones y Estudios Estratégicos (ANEPE)*, nº 6, 2021.

[31] 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

having to resort to the use of force, which is prohibitively expensive in economic and social terms and always has uncertain consequences"[32].

These actions can be "significant enough to destabilize regions and affect global security"[33], which can serve to "prepare at all levels—social, ideological, logistical, communicative, intelligence gathering, sometimes economic, etc.—the stage for a future war or, also, to be an instrument of interference in the dynamics following an armed conflict "the stage for a future war or also to be an instrument of interference in the dynamics following an armed conflict[34].

Based on all of the above, it is legitimate to question the ultimate goal of Russia's use of the gray zone against NATO. Is it seeking to obtain geopolitical gains? Is it seeking to create conditions for post-conflict management in Ukraine? Or is it setting the stage for a new and greater war in Eastern Europe? From a liberal-institutionalist perspective, these dynamics could be interpreted as a problem of insufficient mechanisms for transparency, verification, and governance in the gray zone, where the cost of opportunistic action is low and attribution is difficult. For its part, a constructivist approach would emphasize the weight of identity narratives, historical frameworks, and mutual perceptions of threat that facilitate social acceptance of revisionist behavior. However, from a neorealist framework, the gray zone is the privileged arena in which revisionist powers such as Russia attempt to maximize their security and alter the balance of power without assuming the costs of armed conflict with NATO.

This paper adopts neorealism as its main framework because it best explains the structural logic of competition, the security dilemma, and the cost/benefit calculation that encourages the sustained use of hybrid instruments below the threshold of armed conflict. It is important to explore this issue in greater depth, as NATO's Strategic Concept 2022 does not use the term "gray zone," although the concept is implicitly present when it refers to hybrid threats or systemic challenges[35]. With this objective in mind, the following

[32] SOTO SILVA, "La zona gris, un desafío para la conducción política y estratégica", p. 11.
[33] RODRÍGUEZ GÓMEZ, "Conflictos en la zona gris; la nueva amenaza universal", p. 2.
[34] BAQUÉS, "Hacia una definición del concepto «Gray Zone» (GZ)", pp. 15-16.
[35] NATO, *Strategic Concept 2022*, 2022, disponible en https://www.nato.int/en/about-us/official-texts-and-resources/strategic-concepts/nato-2022-strategic-concept

section outlines some of the hybrid instruments that the Kremlin has been using against NATO member countries over the last few decades.

2. Russian hybrid instruments in the gray zone in the confrontation with NATO

The collapse, dismemberment, and disappearance of the Soviet Union in 1991 gave way to a Russia with diminished and meager capabilities in the face of severe economic, social, political, and ethnic problems. With President Yeltsin in the hands of powerful oligarchs—especially as his health deteriorated— the 1990s were traumatic for the Russian people, with internal humiliations—defeat in the first Chechen war (1994-1996)—and external ones—the bombing of its ally Serbia during the Kosovo war (1999). Therefore, since his arrival as prime minister on August 9, 1999, and later, on December 31 of the same year, as president of the country, Vladimir Putin sought to restore national pride, achieving a series of successes in his early years in office—overcoming the economic crisis of the late 1990s, victory in the Second Chechen War, subjugation of the oligarchs, etc.

On the foreign front, the capabilities of the Russian state could not be compared to those of the United States, the growing European Union, or the emerging China, so it regularly resorted to the use of hybrid instruments—less costly than conventional ones and adaptable to the new realities of the 21st century—to strengthen and increase its position in the post-Cold War international political system, especially in the so-called “near abroad,” the geopolitical space made up of the former Soviet republics and their surroundings.

Ukraine, although not a member of NATO, is undoubtedly the epitome of Russia's use of hybrid instruments beyond its borders and therefore deserves to be discussed as an example of the Kremlin's strategies and actions. During the 2004 election campaign, one of the presidential candidates, Viktor Yanukovych, received significant political and media support from Moscow, as well as advisors. However, the Orange Revolution brought the pro-Western Yushchenko to the Ukrainian presidency, which meant that over the following years the country suffered constant pressure from Russia, including

confrontation over gas prices, media pressure, and cyberattacks. All of this contributed to the failure of Yushchenko's presidency, paving the way for Yanukovych's electoral victory in the new elections in 2010. The Kremlin seemed to have won the game, but the stagnation of the Ukrainian state, the multifactorial crisis, and endemic corruption, coupled with the polarization between pro-Western and pro-Russian factions, led to the events of late 2013 and early 2014. Yanukovych fled the country and a government much closer to Brussels than to Moscow was established. Putin's reaction was swift.

During the political crisis that was ravaging Ukraine, Russia sent additional troops to its bases in Crimea under the 1997 Partition Treaty[36]. Then, in February, uniformed and armed soldiers, but without insignia, claiming to be self-defense militias against Kiev, set up checkpoints in Armyansk and Chongar, the two main road junctions between mainland Ukraine and the Crimean Peninsula[37]. Gradually, these supposed militias occupied key infrastructure on the peninsula. The result of these actions was that the pro-Russian part of the area consolidated territorial and operational control of access points and began a process of separation and independence. In March, taking advantage of this scenario, a referendum was held asking whether they wanted the Republic of Crimea to join Russia. According to the Electoral Commission, 96.77% of voters were in favor of incorporating this territory into Russia[38]. As a result, the Russian Federation succeeded in annexing Crimea, despite condemnation from the vast majority of the international community.

The Kremlin also focused its attention on Donetsk and Luhansk, eastern provinces of Ukraine populated mainly by citizens of Russian origin who settled in the territory during Stalin's time. Clashes between self-proclaimed “self-defense militias” and the Ukrainian army led to the Kremlin's covert involvement in the conflict. In addition to providing logistical, military, and economic support to the pro-Russian rebel authorities and their militias, Russia directly involved thousands of its professional soldiers—including special

[36] In 1997, a comprehensive treaty between Russia and Ukraine affirmed the integrity of Ukraine's borders, something that Russia and the Western nuclear powers also guaranteed in the 1994 Budapest Memorandum, when Ukraine agreed to surrender its Soviet-made nuclear arsenal. See https://www.bbc.com/mundo/noticias-internacional-60237751

[37] 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

[38] 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

forces—although always passing them off as members of the local forces. There is also evidence that it deployed portable anti-aircraft missiles and heavy artillery on the ground, as well as other types of unconventional artillery: aerial drones. Among the models provided to the forces deployed in the rebel provinces, the use of Granat 1 and 2, ZALA 421–08, Eleron 3SV, and Zastava was observed[39]. The use of this type of weaponry allowed the Moscow-backed rebels to inflict heavy casualties on the Ukrainian side, while keeping separatist casualties to a minimum.

Ukraine illustrates how sustained pressure in the gray zone can alter strategic balances without explicitly crossing the threshold of armed conflict. Thus, operational ambiguity reduces the expected costs of action and hinders the coordination of deterrence, while, from the perspective of offensive realism, these practices maximize opportunistic gains in favorable time windows. This pattern is relevant because it anticipates the logic of using hybrid instruments in environments where the adversary does have collective defense commitments.

In addition to the armed confrontation that Russia was promoting in a more or less veiled manner in eastern Ukraine, between 2014 and 2022 there were a series of unconventional attacks whose authorship points to the Kremlin. In 2014, the Snake cyberespionage malware—also known as Ouroboros—attacked and infected numerous computer networks in Ukraine. This malware turned out to be very similar to one that had previously attacked the US Pentagon's systems. In fact, the Snake virus also attacked Lithuania, the United Kingdom, and Georgia[40].

In 2016, a cyberattack was successfully carried out that left Kiev without electricity for an hour. This cyberattack was carried out by spear-phishing—social engineering—and, according to the US Department of Homeland Security, approximately 80,000 customers of the utility company Prykarpattyaoblenergo were affected in western Ukraine[41].The

[39] JORDÁN, J, "Algunas lecciones del combate terrestre en el Donbass", *Global Strategy*, 2019, disponible en https://global-strategy.org/algunas-lecciones-del-combate-terrestre-en-el-donbass-2014-2015-artilleria-fuerzas-acorazadas-y-mecanizadas/

[40] 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

[41] 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

incident demonstrated Ukraine's vulnerability to this type of cyberattack, whose benefits in the 21st century can far outweigh the minimal costs. In fact, as early as 2007, Estonia, following the removal of a Soviet-era monument, had suffered a wave of DDoS (Distributed Denial of Service) cyberattacks that sought to overwhelm the systems of banks, ministries, the media, and parliament[42]. In 2015, a cyberattack blocked the broadcasts of several TV5Monde channels. Although initially claimed by an alleged jihadist group, subsequent investigations by the French government attributed the attack to Russia's GRU (military intelligence). Also in that same year, an unauthorized intrusion into the German parliament's network was detected, for which a member of APT28, a group of hackers linked to the GRU, was blamed.

Furthermore, the Czech and Bulgarian intelligence services accused the GRU—Russia's military intelligence agency—of being responsible for explosions at ammunition depots in the Czech Republic and Bulgaria between 2014 and 2015 with the aim of hindering the supply of weapons to Ukraine. The strategic objective is not only to influence specific decisions, but also to erode the cohesion of NATO member countries and increase their internal uncertainty. If the political and social costs of maintaining a firm stance are perceived to be increasing, the capacity for coordination diminishes and deterrence is undermined. In other words, the logic of the gray zone does not lie in decisive victories, but in the progressive accumulation of political, social, and strategic costs for the adversary.

Based on the above, it is noteworthy that the Kremlin has given direct or indirect support to a whole series of political parties throughout Europe, such as Marine Le Pen's National Rally (formerly the National Front) in France, the AfD in Germany, the Lega in Italy, the FPÖ in Austria, Fidesz in Hungary, and so on[43]. Various parliamentary and journalistic investigations have exposed irregular financing schemes involving members of these

[42] GRASSEGER, Hannes y KROGERUS, Mikael, “Fake news, botnets and how Russia weaponised the web”, *The Guardian*, 2 de diciembre de 2017, available at the following link https://www.theguardian.com/technology/2017/dec/02/fake-news-botnets-how-russia-weaponised-the-web-cyber-attack-estonia

[43] BOYLE, Catherine, “Russian links to EU far right exposed by French loan”, *CNBC*, 25 de noviembre de 2014, available at the following link https://www.cnbc.com/2014/11/25/russian-links-to-eu-far-right-exposed-by-french-loan.html; 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

parties, relationships with Kremlin envoys, and a constant presence in pro-Russian media outlets.

Also noteworthy are the hybrid campaigns carried out in Baltic and Central Europe, where Eurosceptic forces have received constant support through companies and societies linked to the Kremlin[44]. During the 2016 US election campaign, a series of events seemed to favor the Republican presidential candidate: the hacking and subsequent leaking of emails from the Democratic National Committee and Hillary Clinton's campaign, the use of platforms such as WikiLeaks to selectively disseminate damaging information, and the massive use of bots and trolls on social media to amplify content in favor of one of the candidates and polarize the campaign[45].

In 2016, on election day, the security forces of Montenegro, then a NATO candidate, foiled a plot to storm the parliament, kill the prime minister, and install a pro-Russian government during the parliamentary elections. The courts convicted several Montenegrin citizens and Russian agents. In 2016 in Moldova, pro-Russian Igor Dodon of the Party of Socialists (PSRM) won the presidential election. He then visited Moscow. Since then, Russia, through the GRU and the FSB, has financed the PSRM and pro-Russian networks in the country and used funds for campaigns and protests.

In 2017, shortly before the second round of the French presidential elections, there was a massive theft and leak of documents from Emmanuel Macron's campaign. Various investigations pointed to an operation by the APT28 group linked to the GRU. Throughout the 2010s, Russia invited and supported the leaders of UKIP and Eurosceptic forces, who were given prominent coverage in Kremlin-friendly international media outlets such as RT and Sputnik. Narratives aligned with Brexit, opposition to sanctions against Russia, and criticism of NATO were promoted[46]. In 2018, former Russian spy Sergei Skripal and his daughter were attacked with the nerve agent Novichok. GRU agents were accused of the

[44] EUVSDISINFO, “Las mentiras de la Plaza Roja: propaganda en el desfile, en Internet y en las calles”, *EUvsDisinfo*, 8 de mayo de 2025, available at the following link https://euvsdisinfo.eu/es/las-mentiras-de-la-plaza-roja-propaganda-en-el-desfile-en-internet-y-en-las-calles/

[45] 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, available at the following link https://www.theguardian.com/world/2017/jan/06/vladimir-putin-us-election-interference-report-donald-trump

[46] BOYLE, “Russian links to EU far right exposed by French loan”.

attack. The Kremlin reacted with a massive disinformation campaign in the media and on social networks.

In 2018, during NATO's Trident Juncture exercise, Norway and Finland reported deliberate interference with the GPS system, blaming Russia for an electronic warfare maneuver that could have disastrous consequences for civil aviation. The EUvsDisinfo unit and the European External Action Service have documented hundreds of massive disinformation campaigns that seek to influence public opinion in NATO member countries, whether on issues related to national elections, referendums, debates, perceptions of Russia, migration, values, vaccines, etc.[47]

In 2022, Kiev reported that a group called Sandworm deployed malicious software to destroy and erase data on computers controlling high-voltage substations in Ukraine[48]. Although this attack was not as successful as in 2016, the Russian Federation managed to create uncertainty among the population and pave the way for a new phase of the conflict. In February 2022, Putin, insisting that this was neither a war nor an invasion, but rather a special military operation to defend the Russian-speaking population and denazify the neighboring country, and as part of a broad hybrid strategy of communication, disinformation, and cyberattacks, ordered the invasion of Ukraine[49].

With the start of the Russian invasion of Ukraine in February 2022, the Kremlin combined conventional warfare strategies with hybrid instruments in a broad-spectrum campaign aimed not only at subjugating the Ukrainian people, but also at deterring or hindering any possible external aid to Kyiv. In the first case, the systematic and periodic attack with Russian missiles and drones against Ukrainian power plants and substations—civilian infrastructure—especially since the fall of 2022, with the aim of leaving the non-combatant population without power in the face of winter, is undoubtedly a clear violation of international humanitarian law. On the other hand, there have been reports of constant

[47] EUVSDISINFO, “Las mentiras de la Plaza Roja: propaganda en el desfile, en Internet y en las calles”.

[48] REUTERS, “Hackers rusos intentaron sabotear la red eléctrica ucraniana -autoridades e investigadores”, *Euronews*, 12 de abril de 2022, available at the following link https://es.euronews.com/2022/04/12/ucrania-crisis-ciber

[49] CUETO, J. C., “Rusia y Ucrania: así acabaron otras incursiones militares ordenadas por Putin”, *BBC*, 6 de marzo de 2022, available at the following link https://www.bbc.com/mundo/noticias-internacional-60524454; EL PAÍS, “¿Cuál es el origen del conflicto entre Rusia y Ucrania?”, *El País*, 1 de marzo de 2022, available at the following link https://elpais.com/internacional/2022-03-01/origen-del-ataque-de-rusia-a-ucrania.html

malware attacks—WhisperGate, HermeticWiper, variants of Sandworm—against ministries, banks, and critical infrastructure.

With regard to the hybrid campaign against NATO and EU member states, between 2022 and 2025, around 150 incidents have been detected in infrastructure—minor explosions, suspicious fires, railway sabotage, severed submarine cables, etc.—have been detected, which European authorities have attributed to actors linked to the Kremlin or its proxies, resulting in a significant diversion of resources by the affected countries.

Moldova, a country that hosts more than 1,000 Russian soldiers stationed in the disputed region of Transnistria, has been one of the preferred targets of Russia's hybrid strategies. Investigations by RISE Moldova/OCCRP have exposed the existence of a Russian funding network that supports pro-Russian figures such as Igor Dodon, who was president of the country between 2016 and 2020, as well as like-minded political parties such as the PSRM and the Șor Party. In addition, this funding has also been used to pay for vote buying and incite anti-government and anti-European protests[50].

In 2023, the Șor Party, led from Moscow by fugitive oligarch Ilan Shor, was outlawed by Moldova's Constitutional Court, which considered it a Russian instrument to gain control of the Moldovan state and slow its rapprochement with the European Union. In 2025, Yevgenia Gutsul, one of the leaders of the Șor Party, was sentenced to seven years in prison for illegally bringing money from Russia to finance her political party and pro-Russian protests[51]. In addition, during the 2024 presidential and 2025 parliamentary elections, according to reports by the Moldovan authorities and intelligence services, there was a proliferation of cyberattacks, disinformation campaigns on popular social networks, vote buying, financing of pro-Russian parties, and attempts at violent protests against the pro-European government of Maia Sandu[52].

[50] MCGRATH, S., “Moldova election raids point to Russian interference”, *Associated Press*, 23 de septiembre de 2025, available at the following link https://apnews.com/article/moldova-election-russia-raids-europe-; ROBERT LANSING INSTITUTE, “The Kiriyenko blueprint: Turning Moldova’s election into an operation”, *Robert Lansing Institute*, 25 de septiembre de 2025, available at the following link https://lansinginstitute.org/2025/09/25/the-kiriyenko-blueprint-turning-moldovas-election-into-an-operation/

[51] SAUER, P., “Moldovan regional leader sentenced to seven years in prison over Russian funding”, *The Guardian*, 5 de agosto de 2025, available at the following link https://www.theguardian.com/world/2025/aug/05/moldova-gagauzia-yevgenia-gutsul-sentenced

[52] MCGRATH, S. y GHIRDA, V., “Moldova presidential election marred by corruption and fraud allegations”, *Associated Press*, 3 de noviembre de 2024, available at the following link https://apnews.com/article/moldova-

In addition, the political parties Moldova Mare and Partidul Republican „Inima Moldovei" were prevented from participating in the 2025 legislative elections on charges of having been illegally financed from abroad[53]. The complex case of Romania should also be highlighted. Since 2023, EUvsDisinfo and other observatories have been documenting massive campaigns that seek to impose pro-Russian narratives on social media, whether by relativizing Russian aggression against Ukraine, defaming the EU and NATO, insulting pro-European candidates, etc.[54] This campaign reached its peak during the 2024 presidential elections, when Călin Georgescu, a nationalist, anti-European, and pro-Russian candidate, won a surprise victory in the first round after an intense presence of his messages on social media such as TikTok and Telegram.

The Romanian security services and international media soon reported that Georgescu's candidacy had been supported by a massive disinformation and manipulation operation coordinated from Russia, involving the intensive use of bots, fake accounts, and viral content. This led the Constitutional Court to annul the results, concluding that there had been significant foreign intelligence involvement through cyber operations, the use of bots on social media, irregular financing, etc.[55] Russian actions have also been felt in other NATO member countries. Six foreign nationals are accused in Lithuania of attempting, on behalf of the GRU, to attack TVC Solutions, a supplier to the Ukrainian armed forces, in 2024. They are also suspected of involvement in attacks and attempted attacks on buses, a post office, shopping centers, a cinema, a paper warehouse, and oil and gas infrastructure in the Czech Republic, Romania, and Poland[56].

presidential-election-russia-corruption-fraud-5886447779a4a818e9f30fdadcb8bbe5; 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/

[53] CAMINO, J., "Moldova bans pro-Russia party from parliamentary elections", *DW*, 26 de septiembre de 2025, available at the following link https://www.dw.com/en/moldova-bars-pro-russia-party-from-parliamentary-elections/a-74153073; REUTERS, "Kremlin denies interference in Romanian election", *Reuters*, 29 de noviembre de 2024, available at the following link https://www.reuters.com/world/europe/kremlin-denies-russian-interference-romanian-election-2024-11-29/

[54] EUVSDISINFO, "Las mentiras de la Plaza Roja: propaganda en el desfile, en Internet y en las calles".

[55] HAECK, P., "TikTok removed 3 influence campaigns during Romania's elections – European Parliament", *Politico*, 3 de diciembre de 2024, available at the following link https://www.politico.eu/article/tiktok-removed-3-influence-campaigns-during-romania-elections-european-parliament/; REUTERS, "Kremlin denies interference in Romanian election", *Reuters*, 29 de noviembre de 2024, available at the following link https://www.reuters.com/world/europe/kremlin-denies-russian-interference-romanian-election-2024-11-29/

[56] AFP, "Lituania acusa a seis extranjeros de terrorismo por atacar ayuda destinada a Ucrania", *La Nación*, 16 de enero de 2026, available at the following link https://www.lanacion.com.ar/agencias/lituania-acusa-a-seis-extranjeros-de-terrorismo-por-atacar-ayuda-destinada-a-ucrania-nid16012026/

Furthermore, in 2024, a cyberattack affected the Danish water company, allowing external manipulation of pump pressure and causing several pipes in the network to burst. In addition, during local elections that same year, there were DDoS cyberattacks against institutional computer systems. In both cases, Danish intelligence accused groups linked to the Kremlin—Z-Pentest and NoName057(16)—of being responsible[57]. The German government recently accused Moscow of being responsible for a series of hostile hybrid actions carried out between 2024 and 2025, targeting air traffic management systems and the German federal elections. The actions were allegedly carried out by the APT28 group, mentioned above[58].

Of particular concern have been violations of NATO member countries' airspace by Russian drones. In July, Lithuania reported that two Russian drones had entered its territory on separate dates, probably due to a technical error that diverted them from their target in Ukraine. On September 8, a Russian drone violated Romanian airspace to attack Ukraine. On September 9, at least 19 Russian drones flew over Polish airspace. The number of unmanned vehicles casts doubt on the technical failure hypothesis, pointing to the possibility that this was an action in the gray zone. On September 13, a Russian drone was shot down in Romania. Two days later, on September 15, another aerial drone was shot down over Warsaw. These incursions prompted the Polish government to invoke Article 4 of the NATO treaty, a rarely used mechanism that is activated when a member is threatened and leads to a formal debate within the Alliance[59].

In parallel with the above incidents, several NATO countries reported the presence of unidentified drones near military bases and civilian airports in late September, severely disrupting air traffic. Denmark saw operations affected at the airports of Copenhagen,

[57] BRYANT, M., “Denmark says Russia behind cyber attacks”, *The Guardian*, 18 de diciembre de 2025, available at the following link https://www.theguardian.com/world/2025/dec/18/denmark-says-russia-was-behind-two-destructive-and-disruptive-cyber-attacks

[58] ISSEL, S., “Alemania acusa a Rusia de ciberataque al control aéreo”, *Euronews*, 12 de diciembre de 2025, available at the following link https://es.euronews.com/2025/12/12/alemania-acusa-rusia-ciberataque-control-aereo-desinformacion-electora

[59] 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, available at the following link https://www.nytimes.com/es/2025/09/10/espanol/mundo/polonia-rusia-drones-ucrania.html

Aalborg, Billund, Esbjerg, and Sonderborg. Days later, the Norwegian airport in Oslo was affected. Other incidents have been reported in France and Germany, with the origin and purpose of the small aerial drones remaining unclear[60]. The harassment of NATO member countries' air infrastructure is complemented by constant interference with GPS (Global Positioning System). The disruption in August 2025 of the charter flight carrying the European Commission from Poland to Belgium highlighted a strategy that has affected thousands of aircraft in recent years, especially those flying over countries bordering Russia or the Russian enclave of Kaliningrad[61].

Also noteworthy are several incidents in the Baltic Sea that have resulted in the cutting of submarine cables vital to various regional infrastructures. In November 2024, the BCS East-West Intelink and C-Lion1 telecommunications cables, connecting Lithuania-Sweden and Germany-Finland respectively, were damaged, with suspicion falling on a Chinese ship that had departed from a Russian port[62]. Shortly thereafter, in December 2024, the Estlink-2 power cable and four telecommunications cables connecting Finland and Estonia were cut or damaged by the oil tanker Eagle S, flying the flag of the Cook Islands but linked to the “ghost fleet” that Russia uses to evade international sanctions.

Finnish authorities boarded the ship and charged the officers with aggravated criminal damage and communications interference[63]. Finally, on December 31, 2025, the Elisa submarine telecommunications cable connecting Finland and Estonia was damaged by the cargo ship Fitburg, flying the flag of Saint Vincent and the Grenadines, which had departed from the Russian port of Saint Petersburg. Finnish authorities boarded the ship

[60] 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, available at the following link https://es.euronews.com/next/2025/09/30/del-baltico-al-mediterraneo-la-incursion-de-drones-en-paises-europeos-pone-en-alerta-a-la-

[61] AYUSO, S., “El avión en el que viajaba Von der Leyen sufre interferencias rusas en el GPS”, *El País*, 1 de septiembre de 2025, available at the following link https://elpais.com/internacional/2025-09-01/el-avion-en-el-que-viajaba-von-der-leyen-sufre-interferencias-rusas-en-el-gps.html

[62] ASTIER, H. y KIRBY, P., “Undersea cables severed in Baltic Sea raise security concerns”, *BBC*, 19 de noviembre de 2024, available at the following link https://www.bbc.com/news/articles/c9dl4vxw501o

[63] LEHTO, E. y SYTAS, A., “Finland boards oil tanker suspected of causing internet, power cable outages”, *Reuters*, 26 de diciembre de 2024, available at the following link https://www.reuters.com/world/europe/finland-police-investigate-role-foreign-ship-after-power-cable-outage-2024-12-26/

and launched an investigation into aggravated criminal damage and telecommunications interference[64].

In summary, this section has presented a non-exhaustive selection of events attributed—or likely to be attributed—to the Russian Federation that have directly or indirectly affected the national and collective security of NATO member countries. The actions presented can be organized in the following typological table:

Types of hybrid activities carried out by Russia in Ukraine and in NATO's gray zone			
Nº	**activity category**	**Description**	**Objective**
1	Cyberattacks	Attacks on critical infrastructure. DDoS, *hack and leak*.	Degradation, signage, and reputational and material costs.
2	Misinformation / Influence	Sustained campaigns, bots, manipulation of platforms and media and social media.	Political and social polarization and erosion of trust in institutions.
3	Recruitment and political coercion	Support for pro-Russian parties and networks, influence buying.	Modify internal preferences and policies.
4	Sabotage of critical infrastructure	Fires, explosions, underwater cable cuts.	Economic cost and demonstrating vulnerability.
5	Military pressure that is not attributable or has little cost	Drones, airspace violations, GPS interference.	Threshold setting and risk calculation.

[64] POHJANPALO, K., "Finlandia toma un buque por causar daños a cable submarino de telecomunicaciones", *El Financiero*, 31 de diciembre de 2025, available at the following link https://www.elfinanciero.com.mx/mundo/2025/12/31/finlandia-toma-un-buque-por-causar-danos-a-cable-submarino-de-telecomunicaciones/

6	Use of proxies	Interposed parties, plausible denial.	Avoid triggering defense mechanisms.

Table 1. Own elaboration. Types of hybrid activities carried out by Russia in Ukraine and in NATO's gray zone.

This typology shows that the common logic is not to achieve immediate victory, but rather to generate cumulative friction on three critical variables of deterrence—capacity, determination, and communication—gradually undermining allied credibility without crossing the threshold of armed conflict.

Moscow's systematic use of this type of action highlights the existence of a confrontation between Russia and NATO, which, fortunately, has not yet reached the intensity threshold of an international armed conflict. The strategies and instruments developed by Russia in the gray zone of confrontation, whether they seek to obtain geopolitical gains without resorting to war or to set the stage for the start of a localized armed conflict, are, and this is a fact, a threat to the national security of neighboring countries, to the collective security of NATO, and to the principles of international law on which the system of nations that emerged after World War II is based. Thus, NATO member countries must be aware of the situation and act accordingly.

3. Deterrence: a key element in the prevention of armed conflict

Beyond their diversity, the facts set out above respond to the same logic: to gradually and systematically erode the existing conditions of deterrence. Therefore, it is pertinent to analyze the effects that these have produced on the Alliance and what instruments allow for denying benefits or imposing costs without provoking an armed escalation.

So far, NATO's response has not been unanimous or adequate. Regarding the former, Hungary with Orbán, Turkey with Erdoğan and the United States with Trump have been continually reticent—or contradictory—to certain commitments, including that implied by Article 5 of the North Atlantic Treaty referring to the principle of collective defense. With regard to the latter, since the beginning of the Russian aggression against Ukraine, NATO has activated its defense plans, deploying land, air, and sea forces in Eastern Europe. High-readiness elements of the NATO Response Force were employed, placing more than 40,000 personnel under direct Allied command, supported by additional national deployments. In addition, in March 2022 the Alliance agreed to create four new

multinational battle groups in Bulgaria, Hungary, Romania and Slovakia, joining the existing ones in Estonia, Latvia, Lithuania and Poland[65]. However, these measures, although limited, have a preventive character for a scenario of conventional armed conflict, but do not represent an instrument to face a confrontation in the gray area.
Thus, for example, shooting down cheap Russian drones that venture into NATO airspace with expensive air-to-air missiles fired from expensive F-35 or Eurofighter Typhoon fighter jets is not sustainable or appropriate. Faced with this, the authors agree that NATO member countries must make significant efforts to restore a fundamental instrument in the prevention of armed conflicts: deterrence.

According to Jordan[66], "deterrence is a relational variable, the result of an interaction in which the deterred chooses not to carry out an action, which they would otherwise carry out, by estimating the costs that it may entail". Thus, the objective of the actor that would exercise deterrence —NATO— is to influence the calculation of risks and benefits of the other party —Russia— to deter it from taking a certain action. Deterrence can be exercised through denial —hindering action or minimizing profits— or retaliation —maximizing costs through punishment—, being able to resort to a wide range of instruments: military threats, diplomacy, economics, information, sanctions, etc[67].

If the actors conclude that the benefits of attacking first do not merit the costs to be incurred, a strategic stability is achieved that removes the possibility of an armed conflict[68]. To this principle we must add the inclusion of guarantees, since, although "deterrence is based on threats associated with crossing certain limits", it must also "alleviate the insecurity of the other party by guaranteeing that it has nothing to fear if it respects them"[69], thus seeking to avoid falling into the pernicious dynamics of the security

[65] NATO, *Strategic Concept 2022*, pp. 15 - 16.
[66] JORDÁN, J., "La disuasión en la zona gris: una exploración teórica", *Revista Española de Ciencia Política*, nº 59, 2022, pp. 65-88.
[67] FREEDMAN, L., *Deterrence*, Polity Press, 2004; JORDÁN, J., "La disuasión en la zona gris: una exploración teórica", *Revista Española de Ciencia Política*, nº 59, 2022, pp. 65-88; KNOPF, J. W., "The fourth wave in deterrence research", *Contemporary Security Policy*, vol. 31, nº 1, 2010, pp. 1-33, available at the following link https://doi.org/10.1080/13523261003640819; SNYDER, G. H., *Deterrence and Defense: Toward a Theory of National Security*, Princeton University Press, 1961.
[68] 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*, nº 59, 2022, pp. 65-88.
[69] JORDÁN, "La disuasión en la zona gris: una exploración teórica", p. 71.

dilemma. Finally, particularly in the case of Russia, a concept developed in the last two decades is relevant: tailor-made deterrence, which implies "knowing in depth the values, norms, interests and conditioning factors of those who make decisions to understand their mentality or strategic culture"[70], thereby forcing the disciplinary expansion of the analysis of the actor. Must of the academic literature on deterrence comes from the Cold War and is thought of from a conventional and bipolar perspective.

Its application in a confrontation that takes place in the gray zone is not without problems, especially in the face of those actions that carry few risks for the aggressor - for example, cyber attacks - are difficult to prevent - denial - and complex to retaliate for fear of provoking an escalation towards armed conflict[71]. Thus, Jordan warns of two major problems for effective deterrence in the gray zone. The first is that it is "doubtfully effective" at low intensity thresholds, while it is "more likely to succeed" at high ones. The second, that, in the gray area, characterized by being a volatile, uncertain, complex and ambiguous area, it is tremendously difficult to control the escalation of the confrontation[72]

In addition to the authors mentioned, the authors want to highlight a third: the absence of a sufficient legal framework to regulate a confrontation in the gray zone. Since it does not reach the category of an armed conflict, neither International Law on self-defense —ius ad bellum— nor International Humanitarian Law —ius in bello— applies to the issue, and actions in this scenario must be guided solely by International Human Rights Law. This, in the case referring to Russia and NATO, creates a "legal asymmetry," as Western governments are more dependent on public opinion criticism regarding their actions and this limits their response capabilities[73]. Thus, it seems that Russia, due to its geopolitical characteristics, holds a significant advantage over NATO in the confrontation taking place in the gray zone. However, it depends on the NATO member countries and their societies whether this advantage is circumstantial and not structural. Unlike classical deterrence, which focuses on preventing the outbreak of armed conflict, gray zone deterrence seeks to modulate behaviors, establish tacit limits, and manage escalation within the context of

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

ongoing competition.

Effective deterrence is based on credibility, "understood as the perceived probability that the deterrent will materialize its threat when the conditions that are supposed to activate the deterrence are met"[74]. This depends on three factors: capability —material resources to defend or retaliate—, determination —political will to employ the capabilities—, and communication —effective to be credible—.

It is noteworthy that these three factors do not add up, but rather multiply[75]. Therefore, low values in one of them undermine the effectiveness of deterrence. According to Jordán[76], an effective deterrence strategy must be "non-escalatory, tailored and offering guarantees, based on credibility derived from capabilities, determination, and communication adapted to the gray zone, and assume that it is cumulative deterrence." Regarding the latter, Jordán states that deterrence in the gray zone is "a result of multiple unfriendly interactions where the deterrent can impose itself and convey the need to respect certain boundaries." Cumulative deterrence de facto assumes the repeated failure of both general deterrence and immediate deterrence. However, it seeks to achieve strategic stability through a learning process where norms of conduct, sometimes known as "rules of the game," take shape[77].

From NATO's perspective and based on the purposes and principles of the Strategic Concept 2022, deterrence by denial must be based on resilience, integrated deterrence, and an approach that involves the entire society. The experience of Ukraine has demonstrated the importance of this approach, as the resilience of the Ukrainian people "it is structured around a combination of numerous forms and practices of resilience as a social characteristic of self-sufficiency, autonomy, and self-organization." […]. It is a hybrid resilience based on a form of decentralized governance, the sustainability of social networks, reliable information policy, and a firm public adherence to the idea of a just war. [...] It is hybrid resilience that is the essential point of Ukraine's survival as a nation[78].

[74] JORDÁN**,** "La disuasión en la zona gris: una exploración teórica", p. 69.
[75] Ibíd., p. 69.
[76] Ibíd., pp. 78 – 82.
[77] Ibíd., p. 82.
[78] KURNYSHOVA, Y. y MAKARYCHEV, A., "La guerra de Rusia y la sociedad ucraniana", en *Amenazas híbridas, orden vulnerable*, *CIDOB Report*, nº 08, CIDOB, 2022, pp. 47-54.

Thus, NATO's deterrence by denial aims to increase allied resilience by, through strategies of structural prevention, vulnerability reduction, and denial of strategic advantages, denying strategic benefits to hostile actors. On the other hand, and also in line with the *Strategic Concept 2022*, deterrence through retaliation by NATO member countries must be based, beyond conventional military instruments, on the imposition of coordinated and proportionate costs through multisectoral sanctions, public attribution, coordinated responses, reputational costs, legal and diplomatic measures.

To illustrate the above claims, and without seeking to be exhaustive but rather to provide an overview of possible mechanisms of denial and retaliation deterrence against hybrid activities in the strategic competition environment of the gray zone, a table has been drawn up based on academic literature by various authors such as Jordan[79], Mearsheimer[80], Kofman and Rojansky[81], Renz and Smith[82], Hoffman[83], Mazarr[84], and Nye[85]. In line with the Strategic Concept 2022, deterrence mechanisms against hybrid activities are based on a combination of resilience, prevention, and the imposition of coordinated costs, seeking to strengthen the allies' ability to deny strategic benefits to hostile actors and respond in a proportionate and legal manner, avoiding armed escalation and preserving strategic stability in a context of systemic competition.

The aim is to combine a neorealist framework with a systematic mapping of the most recurrent hybrid activities and their translation into deterrence mechanisms applicable in the gray zone and aligned with NATO's Strategic Concept 2022. Hybrid activities in the strategic competition environment of the gray zone and possible deterrence mechanisms through denial and retaliation.

[79] JORDÁN, J., "La disuasión en la zona gris: una exploración teórica", *Revista Española de Ciencia Política*, nº 59, 2022, pp. 65-88; JORDÁN, J., "El conflicto internacional en la zona gris", *Revista Española de Ciencia Política*, nº 48, 2018, pp. 129-151, disponible en https://doi.org/10.21308/recp.48.05.
[80] MEARSHEIMER, J. J., *The Tragedy of Great Power Politics*, W. W. Norton, 2001
[81] KURNYSHOVA y MAKARYCHEV, "La guerra de Rusia y la sociedad ucraniana"
[82] RENZ, B. y SMITH, H., *Russia and Hybrid Warfare – Going Beyond the Label*, Aleksanteri Papers, 2016.
[83] HOFFMAN, F. G., *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, 2007
[84] MAZARR, M. J., *Mastering the Gray Zone*, RAND Corporation, 2015.
[85] NYE, J. S., *The Future of Power*, PublicAffairs, 2011.

Hybrid activities in the strategic competition environment of the gray zone and possible mechanisms of deterrence by denial and retaliation			
Nº	**Hybrid activities**	**Deterrence Mechanisms by Denial**	**Retaliation Deterrence Mechanisms**
1	Cyber operations against critical infrastructure	Allied cyber resilience, system redundancy	Public attribution and sanctions
2	DDoS attacks on public institutions	Resilient digital infrastructure	Legal countermeasures and sanctions
3	Robbery and information dissemination operations (*hack and leak*)	Data protection and cyber hygiene	Judicial processes and sanctions
4	Interference in electoral processes	Electoral Protection and Strategic Communication (*StratCom*)	Sanctions and political restrictions
5	Sustained strategic disinformation	Media literacy and early detection	Restrictions on state media
6	Deliberate information saturation (*information flooding*)	Institutional verification and communication capabilities	Coordinated attribution
7	Algorithmic manipulation on social media	Platform regulation	Fines and regulatory blocks

8	Use of generative AI for cognitive operations	AI Governance and Technical Detection	Technological sanctions
9	Covert support for political parties or movements	Financial transparency	Individual sanctions
10	Instrumentalization of ethnic minorities	Protection of rights and social inclusion	OSCE missions and sanctions
11	Transnational pressure on diasporas	Police and consular protection	Personal sanctions
12	Revisionist historical narratives	Public diplomacy and strategic education	Multilateral condemnations
13	Rhetorical nuclear threats	Allied strategic communication	Diplomatic isolation
14	Provocative air incursions	Integrated surveillance and adequate denial mean	Diplomatic protests and sanctions
15	Ambiguous maritime incursions	Maritime situational awareness	Sanctions and non-recognition
16	Covert sabotage of submarine cables	Monitoring and redundancy	Attribution and sanctions
17	Interference in global satellite navigation systems	Alternative systems and protection	Diplomatic measures
18	Use of unidentified irregular forces	Administrative control of the territory	No legal recognition
19	Covert support to armed proxies	Police and border cooperation	Designation and sanctions

20	Covert militarization of civilian spaces	Legal inspections	Multilateral sanctions
21	Selective energy coercion	Energy diversification	Sectoral sanctions
22	Induced dependence on critical resources	Diversification and reserves	Defensive trade measures
23	Selective economic coercion	State support and diversification	Economic sanctions
24	Strategic dumping in key sectors	Legal commercial defense	Countervailing duties
25	Interference in supply chains	Control of strategic dependencies	Defensive measures to eliminate interference
26	Use of private companies as state instruments	Investment control	Asset freeze
27	Fragmented hostile takeovers	Investment evaluation and supervision	Legal blockade
28	Economic and technological espionage	R+D+I Protection	Expulsions and sanctions
29	Covert financial destabilization	Macroprudential supervision	Regulatory measures
30	Pressure on insurance and rating markets	Financial regulation	Coordinated responses
31	Strategic lawfare	Specialized legal capacities	International litigation

32	Deliberate blockade of international organizations	Multilateral coordination	Political isolation
33	Regulatory capture in technical organizations	Active institutional presence	Multilateral challenge
34	Strategic delay in legal mechanisms	Procedural reform	Diplomatic pressure
35	Use of NGO´s or front organizations	Funding control	Legal cancelation
36	Instrumentalization of migration crises	Cooperative border management	Diplomatic and economic sanctions
37	Strategic use of visas and mobility	Consular coordination	Reciprocal measures
38	Instrumentalization of tourism	Economic diversification	Selective restrictions
39	Gradual normalization of illegal fait accompli	Constant institutional presence	Policy of non-recognition
40	Systematic erosion of trust in democratic institutions	Integral resilience of society	Prolonged imposition of costs

Table 2. Own elaboration. Hybrid activities in the strategic competition environment of the gray zone and possible mechanisms of deterrence by denial and retaliation.

In reference to the table, it is worth noting that the denial deterrence mechanisms listed in the table align with NATO's approach of strengthening resilience, aiming to reduce the political, economic, social, and technological vulnerabilities that hostile actors exploit through hybrid activities. Moreover, the retaliation deterrence mechanisms mentioned do not involve the use of armed force, but rather the coordinated imposition of political, economic, legal, and reputational costs among the allies. Thus, both denial and reprisal mechanisms are deliberately positioned below the threshold that would activate Article 5, but within Article 4 where "the Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence, or security of any of the Parties is threatened"[86], favoring coordinated responses.

Thus, in the face of Russian actions in the gray zone, and despite the challenges they pose, it is possible to oppose adequate mechanisms of deterrence through denial or reprisal. However, the big question is whether NATO member countries will collectively articulate capacity, determination, and communication to build a truly credible deterrence.

Conclusions

The analysis developed throughout this work demonstrates that the relationship between Russia and NATO cannot be adequately understood if it is limited to a binary and dichotomous reading between war and peace. For more than two decades, the Kremlin has been deploying a sustained strategy of strategic competition below the threshold of international armed conflict, first in its so-called "near abroad" and, increasingly, against NATO member countries. This dynamic, which fully falls within what specialized literature has conceptualized as the gray zone, today constitutes a direct threat to the national security of member states and to the collective security of the Atlantic organization.

From a neorealist perspective, Russian behavior responds to a logic of seeking security and revising the international status quo in an anarchic, competitive, and transforming system. However, the systematic use of hybrid instruments not only erodes the principles of International Law and the norms that underpin the international order but also increases the risks of unwanted escalation and miscalculation.

[86] NATO, *North Atlantic Treaty*, 1949, available in the next link https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty

Far from constituting isolated or opportunistic actions, these instruments are part of a coherent and cumulative strategy aimed at weakening allied cohesion, exploiting structural vulnerabilities, and conditioning political decision-making. From Waltz's perspective, the state must ensure sufficient power for its survival and, with that, choose the necessary action to achieve it. This is what Russia has been carrying out since the beginning of the war in Ukraine. Undoubtedly, the new instruments used in hybrid warfare, such as the use of drones, have changed the course of the war since its inception, as well as the various cyberattacks that are becoming increasingly sophisticated.

Therefore, it has become even more complicated to ensure the safety of civilians and military personnel, both in Ukraine and the Russian Federation. These threats cause damage ranging from economic losses of thousands of dollars to multiple human casualties. It is crucial to understand that, in this type of war, any type of power that the State has at its disposal—economic, military, diplomatic, social, or cyber—can be employed. From the Russian perspective, ensuring national security involves protecting its sphere of influence at all costs, using all the capabilities at its disposal. Thus, the so-called gray zone is characterized by being a particularly volatile space.

The empirical study of the cases presented shows that many of the behavioral patterns deployed by Russia against Ukraine before 2022 have been reproduced, with the necessary adaptations, in the NATO environment. The fundamental difference lies in the fact that, while Ukraine was progressively isolated and eroded until the onset of the armed conflict, the allied countries have mechanisms of cooperation, collective capabilities, and institutional frameworks that, if employed coherently and coordinatedly, can prevent the confrontation in the gray zone from escalating into a broader conventional war. However, this potential does not automatically translate into effective deterrence.

The work has shown that traditional deterrence mechanisms, designed to prevent armed conflicts, are insufficient to respond to a confrontation characterized by ambiguity, fragmentation, and the progressive accumulation of hostile actions. Deterrence in the gray zone demands an adapted approach, based on the combination of denial and

retaliation deterrence, the construction of societal resilience, inter-institutional coordination, and the imposition of proportional, credible, and sustained costs over time. It is about modulating behaviors, establishing tacit limits, and managing escalation within a permanent competitive environment.

It is crucial that NATO member countries, and their citizens, understand that the defense of democratic rule of law and collective security is not fought solely in the military realm, but also in the political, informational, economic, technological, and social spaces. The credibility of allied deterrence will ultimately depend on the ability to coherently articulate capabilities, political determination, and clear and unified strategic communication.

Ultimately, the confrontation between Russia and NATO is already underway, although it is mostly taking place in the gray zone. Ignoring this reality or underestimating it is equivalent to repeating distant and recent mistakes with potentially more serious consequences. The awareness sought in this work does not aim to normalize confrontation or abandon the principles of the international order, but rather to recognize the real conditions in which strategic competition is currently structured. Only from that recognition will it be possible to design effective deterrence policies that, paradoxically, contribute to preserving peace and preventing the gray zone from turning into a new international armed conflict in Europe.

Antonio Gil Fons, Sarai Valerdi Macías