Countering Russia's Hybrid Playbook: NATO's Doctrinal Evolution, Gaps, and Policy Responses

Introduction & objectives

Hybrid warfare has been a strategic tool since antiquity, employed to achieve objectives in uncertain conditions. Today, the space between war and peace is increasingly "gray," with hybrid threats—mixing conventional and unconventional means—gaining global importance. Despite research, a gap persists in applied studies on how to identify, analyze, and address these challenges (Kramer & Speranza, 2017).

Therefore, this paper aims to close that gap by defining the conceptual framework of hybrid threats and warfare to clarify the "gray zone" of conflict. It then maps Russia's "hybrid playbook," analyzing the fusion of conventional and unconventional instruments used to complicate detection and achieve strategic aims. Subsequently, the study examines NATO's doctrinal evolution and response mechanisms since 2014. Finally, it offers policy recommendations to address gaps in definition, resilience, and attribution capabilities

Conceptual framework: What are hybrid threats & hybrid warfare?

The term hybrid threats, though not new, gained prominence after Russia's 2014 Crimea campaign. It traces back to the 2006 Lebanon War, where Hezbollah combined guerrilla tactics and advanced weaponry, blurring lines between state and non-state actors (Bachmann & Gunneriusson, 2015). Defining hybrid warfare is not just an academic exercise; definitions shape state perceptions, responses, and the responsible agencies.

Hybrid threats historically involve the use of both conventional and irregular forces. Mansoor (2012) cites roots in the Peloponnesian War and Sun Tzu; Hoffman (2007) emphasizes integration of conventional, irregular, and criminal tools by state/non-state actors; Russia's Georgia (2008) campaign exemplifies this. The Military Balance (2015) expands the concept to coordinated military and non-military tools—diplomacy, information operations, cyberattacks, and economic pressure—emphasizing that non-military means can sometimes yield greater influence than force.

A key challenge is the interchangeable use of terms such as hybrid warfare, hybrid threats despite their core differences. (NATO & PfPC, 2024). Hybrid warfare involves combining conventional and irregular means to counter stronger militaries (Mattis & Hoffman, 2005), while hybrid threats encompass activities outside of the war spectrum—such as cyber operations, disinformation, and proxies—operating in the gray area between peace and war (Hoffman, 2007). Distinguishing these terms is essential for targeted policy: military adaptation for warfighting and whole-of-government resilience for gray-zone challenges (Monaghan, 2019).

To sum up, when it comes to framing the hybrid playbook, the main element of success is the difficulty of detection and attribution. (McGrath,2024) The goal for the aggressor is to infiltrate society and reduce its resilience to achieve its strategic objectives to the greatest extent possible, with the least (if any) conventional military involvement (Traverton et al., 2018). The hybrid arsenal includes a variety of tools,

such as informational, cyber, diplomatic, economic, and legal, as well as the instrumentalization of migration, terrorism, and anything that can be the target's Achilles heel (Aday et al., 2019).

Russia's hybrid playbook

Modern warfare has changed profoundly. As economic ties grew, the cost of open warfare soared. For Russia, which is militarily weaker than the West, this new environment encourages "guerrilla geopolitics." This means fusing conventional and unconventional tools to compete where Russia holds an edge. This approach blends Soviet-era lessons in asymmetric strategy with new technologies that expand reach and precision (Polyakova et al., 2021).

A turning point came in February 2013 when General Valery Gerasimov published "The Value of Science Is in the Foresight" in the Military-Industrial Kurier. He explained that non-military means—information, economic, political, and psychological—matter more than force. Gerasimov proposed a model where conventional military power is secondary and often hidden, while the primary battles are political and cognitive. He argued that surprise, chaos, and ambiguity are key, blurring the line between war and peace. In his words, "wars are no longer declared, and once they have begun, they continue according to an unfamiliar pattern". (Gerasimov, 2016). This logic sets warfare at two linked levels. The first uses non-military tools to destabilize and divide society. The second uses irregular armed groups to seize strategic sites, while hiding their link to the aggressor. These two levels are made to be hard to tell apart. The result is an environment where the victim cannot easily find or stop the attacker. This creates a paralysis of decision-making and blocks joint action—a strategy of controlled chaos (Gerasimov, 2016).

The next strategies of "new-generation warfare" build on this: long non-military campaigns (propaganda, economic pressure, sabotage) to weaken enemy's morale, followed by "electronic knockdown" of infrastructure, and only finally, targeted kinetic actions. Non-military means are central, not secondary (Rácz, 2015).

Nevertheless, it is misleading to treat the so-called Gerasimov Doctrine as a unified, centrally directed Russian grand strategy. The term itself is a Western construct, extrapolated from one article rather than an official policy (Galeotti, 2018). The doctrinal status it is accorded by many Western scholars and institutions is potentially misleading and even dangerous: treating it as the sole blueprint for Russian strategy risks distorting views of Moscow's aims and methods (Renz, 2016). First of all, the idea that Russia demonstrated an innovative war-winning approach in Crimea not only overstates the 'newness' of hybridity in warfare, as has already been discussed at length by several analysts critical of the concept (Galeotti, 2016; Giles, 2016; Popescu, 2015). It also falsely implies the existence of a universal war-winning formula (Renz, 2016). Secondly, Russia's "New Generation Warfare" is not monolithic. It comprises a range of strategic approaches. Gerasimov's article was a response to developments of the Arab Spring risings, the Syrian Revolution, and the so-called "Orange Revolution". Also, the label hybrid warfare anchors analysis to what took place in February 2014 in Crimea, where Gerasimov views was perfectly implied, even as conditions—and

Russian actions—have been changing. Indeed, the hybrid label serves to draw a veil over the conventional aspects of the war in Ukraine. While non-military means of power were deployed, they relied on more traditional conventional measures for their success (Monaghan, 2019).

In practice, Russian strategy reflects a fluid synthesis of ideas, and each shapes outcomes in different ways. Russian intelligence and security services have significant power in Putin's Presidency. Unlike Western agencies, their role has never been solely to gather intelligence but to draw their own conclusions, lobby the government on policy, and carry out direct actions. Assertive, aggressive, and institutionally biased towards cover and political operations, the intelligence agencies have also helped shape Russian notions of modern warfare (Galeotti, 2024). And there is also the military flank. Gerasimov's later statements, including his 2019 address to the Russian Academy of Military Science, emphasized two guiding concepts: limited action and active defense. The former envisions short, focused interventions beyond Russia's borders to defend national interests without overstretch; the latter stresses pre-emptive measures—diplomatic, informational, and military—to neutralize threats before they materialize (Polyakova et al., 2021). This will be part of a pre-conflict period, during which we also see non-military measures employed to weaken the enemy's morale. If the strategy fails, Russia has adopted the old Soviet notion of 'deep battle', giving it a more modern twist by emphasizing artillery and missile fire. This would not be a mass war but a fluid, fast-moving battlefield, through ground, air, sea, and (cyber)space (Galeotti, 2024).

Russia's hybrid strategy is multilayered—starting with propaganda and cyberattacks and escalating to full-scale warfare—but is often misinterpreted (Galeotti, 2024).

NATO's doctrinal evolution and current toolbox

NATO's engagement with hybrid threats began before 2014. As early as 2009–2010, a NATO Capstone Concept flagged hybridity as a growing challenge, highlighting the need to understand the broader environment, address broader access to advanced technologies, and recognize the risk of weapons and high-end capabilities proliferating to non-state actors. The Chechen and Georgian conflicts exposed the wide range of tools Moscow was using to pursue its strategic aims. The way Russia executed the Crimean crisis was a turning point for the Alliance (Galeotti, 2016). It revealed specific capability gaps, such as inadequate strategic communications and insufficient rapid response mechanisms, that NATO needed to address. At the Wales Summit, NATO resolved to confront hybrid challenges across a broad spectrum of military, paramilitary, and political instruments, and to help Allies build resilience. Priority measures included improving strategic communications, conducting hybrid scenario exercises, and strengthening NATO's coordination with other organizations. Consequently, NATO defined hybrid threats as combinations of military and non-military, covert and overt means, from disinformation and cyber-attacks to economic coercion, irregular armed groups, and the use of conventional forces, employed to blur the line between war and peace, complicate decision-making, and achieve rapid, scalable effects. Preparing to prevent, detect, and respond to such campaigns became a top Alliance priority (NATO,2014). The 2022 Strategic Concept integrated hybridity into NATO's three core tasks: deterrence and defense, crisis prevention and management, and cooperative security, reflecting an understanding that hybrid activity

had become a permanent feature of the Euro-Atlantic security environment (NATO,2022).

Doctrinally, NATO's response to hybrid threats rests on a threefold logic of preparation, deterrence, and defense (NATO,2024). In preparation, the Alliance collects, analyses, and shares information to detect and attribute hybrid activity. NATO's Joint Intelligence and Security Division at Headquarters has steadily enhanced its analytic capacity to identify the diverse forms a hybrid campaign can take, while the Alliance serves as a hub of expertise, assisting Allies on request to shore up national resilience. Training, decision-making exercises, and combined civil-military drills are central elements of this preparedness effort, supported by NATO-linked Centres of Excellence such as the StratCom CoE (Riga), the Cooperative Cyber Defence Centre of Excellence (Tallinn), and the Energy Security CoE (Vilnius). Deterrence combines political and military dimensions: politically, by ensuring clear command arrangements and rapid decision-making channels & militarily, by maintaining the ability to deploy appropriate forces at the right time and place. These elements highlight that deterrence is less about threatening retaliation than about convincing adversaries that hybrid methods will not yield strategic dividends. Defence remains the ultimate guarantee, yet its activation in hybrid contexts is complicated by attribution. At the Brussels summit (2018), all members agreed to use Article 5 of the Washington Treaty in the event of a hybrid attack (NATO,2018). However, debates over invoking Article 5 for hybrid attacks underscore the difficulty of attribution and the political complexity of collective action; judgments are likely to remain case-by-case, based on Article 4 (Piella, 2022). The closest change to the logic of Article 5 is the introduction of Counter Hybrid Support Teams that can be directly utilized by a member of the Alliance requesting support, either in a crisis or even to assist in the development of national anti-hybrid capabilities. In November 2019, the first anti-hybrid support team was deployed in Montenegro. Upon request, military advisory teams can be integrated into anti-hybrid support teams, thereby providing a coherent framework of political and military options (NATO, 2024).

Equally significant has been the emphasis on partnerships. NATO has deliberately moved to deepen cooperation with the EU, notably through the EU–NATO Joint Framework on countering hybrid threats and specialized Centres of Excellence such as the Hybrid CoE in Helsinki. Within the EU–NATO dialogue on countering hybrid threats, specific areas of cooperation have been agreed upon. These include threat assessment, strategic communication, cybersecurity, and crisis prevention and response (Καρατράντος, 2019). The EU–NATO framework for countering hybrid threats was formalized in the 2016 Joint Declaration by the Presidents of the European Council and Commission and the NATO Secretary General. The declaration stressed the need for cooperation on resilience, early detection, and prevention, through information sharing and collective responses to hybrid attacks. It also expanded joint exercises to cover the hybrid domain (Pawlak, 2017). On July 10, 2018, the EU and NATO signed a new joint declaration outlining a shared vision for how the two organizations will work together to combat common threats. This new declaration takes stock of EU-NATO cooperation and commits to further deepening it through the Hybrid CoE (NATO, 2023).

Policy suggestions for NATO's reaction to hybrid attacks

A critical observation concerns NATO's adoption of a highly expansive definition of hybrid warfare. The problem is that, by embracing such a broad conceptualization, the definition begins to overlap ideologically with the notion of grand strategy. If hybrid warfare is defined as the use of all available instruments by an actor in pursuit of its objectives, then it ceases to be analytically distinctive; it effectively becomes synonymous with grand strategy, a term that already captures that reality (Caliskan, 2019). The terminological conflation of multiple concepts that broadly describe the same phenomenon reasonably leads to the conclusion that labelling an attack as hybrid does not provide an operational answer regarding specific weapons or capabilities. Consequently, the use of the term in strategic documents risks undermining their credibility (Liaropoulos, 2025). There is, therefore, a danger that the Alliance could become trapped in an ambiguous framework within which it must decide, on a case-by-case basis, whether a given incident constitutes an act of war. Against this backdrop, it is imperative to establish a clear definitional distinction between hybrid threats and hybrid warfare, along with the corresponding instruments required for their effective response.

Countering hybrid attacks requires national resilience and a whole-of-government approach. Hybrid Resilience Cells (HRCs)—cross-sectoral units including key ministries, regulatory authorities, critical infrastructure providers, and civil society—should coordinate vulnerability assessments, crisis management, and liaison with NATO (Rusinaitė, 2025). NATO should also create Hybrid Resilience Networks—secure hubs linking HRCs to standardize crisis communication and mutual assistance. Capacity-building is essential, including mandatory training for HRC staff.

Another major policy shift is to cut off every dependence on critical infrastructure with aggressive actors. The reliance of several European countries, including major powers such as Germany, on Russian energy created dangerous dependencies. A major obstacle to entanglement is that individual states in Europe are smaller and weaker than their adversaries. NATO, together with the European Union, has to provide small states with leverage against hostile actors that they would not otherwise possess (Rusinaitė,2025).

One of the main challenges NATO faces in countering hybrid attacks is the difficulty of attribution — determining with clarity and confidence who is behind an incident. This uncertainty often prevents a collective, timely response, leaving hybrid aggressors to operate in the so-called "grey zone". To address this, NATO should focus on building shared situational awareness, common standards of evidence, and flexible response mechanisms. Strengthening intelligence sharing and analytical cooperation among Allies would enable a faster and more consistent understanding of hybrid incidents. At the political level, NATO should establish clearer thresholds and response options for hybrid activities that fall short of traditional definitions of armed attack, ensuring that, when attribution is established, responses are credible and unified (Bajarūnas, 2025).

Despite criticism of the hybrid attacks concept, the debate has highlighted the need for defensive resilience across the full security spectrum. Hybrid threats show the threat environment is a continuum, and while war's nature remains unchanged, its manifestations evolve with technology. Looking ahead, it is crucial for policymakers to anticipate the emergence of new technologies that can redefine hybrid warfare. As we stand on the brink of advancements such as AI-driven influence operations, the boundaries of hybrid threats may stretch even further. How might these cutting-edge

technologies alter the landscape of global security, and how should NATO adapt to these changes? Ending with this contemplation sets the stage for ongoing innovation and strategic foresight, ensuring readiness for whatever the future may hold (Briant, 2015).

References

1. Kramer, F. D., & Speranza, L. M. (2017, May 30). Meeting the Russian hybrid challenge. Retrieved November 23, 2025, from https://www.atlanticcouncil.org/in-depth-research-reports/report/meeting-the-russian-hybrid-challenge/
2. Bachmann, Sascha-Dominik & Gunneriusson, Hakan. (2015). HYBRID WARS: THE 21st-CENTURY'S NEW THREATS TO GLOBAL PEACE AND SECURITY. Scientia Militaria: South African Journal of Military Studies. 43. 10.5787/43-1-1110
3. Mansoor, P. R. (2012). Introduction: Hybrid Warfare in History. In W. Murray & P. R. Mansoor (Eds.), Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present (pp. 1–17). chapter, Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139199254
4. Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of Hybrid Wars*. Potomac Institute for Policy Studies. https://potomacinstitute.us/images/stories/publications/potomac_hybridwar_0108.pdf
5. Complex crises call for adaptable and durable capabilities. (2015). The Military Balance, 115(1), 5–8. https://doi.org/10.1080/04597222.2015.996334
6. (2024). Hybrid Threats and Hybrid Warfare Reference Curriculum. NATO & PfPC 13-19 https://www.pfp-consortium.org/news/new-hybrid-warfare-reference-curriculum-released-nato-and-pfpc
7. Mattis, J. N., & Hoffman, F. G. (2005). Future Warfare: The Rise of Hybrid Wars. *Proceedings*, *Vol. 131/11/1,233*(Nov. 2005) https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars
8. Monaghan, S. (2019, October 4). Countering Hybrid Warfare So What for the Future Joint Force? *PRISM*, *Vol.8 No.8*. https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf?ver=2019-09-17-231051-890
9. McGrath, S. (2024). Spotlight on the shadow war: Inside Russia's attacks on NATO territory. Commission on Security and Cooperation in Europe. https://www.csce.gov/wp-content/uploads/2024/12/Spotlight-on-the-Shadow-War-Website.pdf
10. Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). Addressing hybrid threats. Swedish Defence University, Center for Asymmetric Threat Studies (CATS), & European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). https://www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf
11. Aday S., Andžāns M., Bērziņa-Čerenkova U., Granelli F., Gravelines J., Hills M., Holmstrom M., Klus A., Martinez-Sanchez I., Mattiisen M., Molder H., Morakabati Y., Pamment J., Sari A., Sazonov V., Simons G., Terra J. (2019). Hybrid Threats. A Strategic Communications Perspective. Riga: NATO

Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/hybrid-threats-a-strategic-communications-perspective/79
12. Polyakova, A., Boulègue, M., Chatterje-Doody, P., Solodkyy, S., Stoicescu, K., & Zarembo, K. (2021). The evolution of Russian hybrid warfare. Center for European Policy Analysis. https://cepa.org/wp-content/uploads/2021/01/CEPA-Hybrid-Warfare-1.28.21.pdf
13. Gerasimov, V. (2016). The value of science is in the foresight: New challenges demand rethinking the forms and methods of carrying out combat operations. Military Review, 96(1), 23–29. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf
14. Rácz, A. (2015). Russia's hybrid war in Ukraine: Breaking the enemy's ability to resist (FIIA Report 43). Finnish Institute of International Affairs. https://www.fiia.fi/wp-content/uploads/2017/01/fiiareport43.pdf
15. Galeotti, M. (2018, March 5). I'm sorry for creating the 'Gerasimov Doctrine'. Foreign Policy. https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/
16. Bettina Renz (2016) Russia and 'hybrid warfare', Contemporary Politics, 22:3, 283-300, DOI: 10.1080/13569775.2016.1201316
17. Galeotti, M. (2024). *Putin's wars: From Chechnya to Ukraine*. Osprey Publishing. https://www.ospreypublishing.com/uk/putins-wars-9781472847553/
18. Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? Small Wars & Insurgencies, 27(2), 282–301. https://doi.org/10.1080/09592318.2015.1129170
19. North Atlantic Treaty Organization. (2014, September 5). Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2014/09/05/wales-summit-declaration
20. North Atlantic Treaty Organization. (2022, June 29). NATO 2022 Strategic Concept. https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf
21. North Atlantic Treaty Organization. (2024, May 7). Countering hybrid threats. https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats
22. North Atlantic Treaty Organization. (2018, July 11). Brussels Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2018/07/11/brussels-summit-declaration
23. Piella, C. G. (2022). NATO's strategies for responding to hybrid conflicts. In P. Bargués, M. Bourekba, & C. Colomina (Eds.), Hybrid threats, vulnerable order (CIDOB Report #08, pp. 47–52). CIDOB. https://www.cidob.org/sites/default/files/2024-06/47-52_GUILLEM%20COLOM%20PIELLA_ANG.pdf
24. Καρατράντος, Τ. (2019). Εξωτερικές σχέσεις και πολιτικές αντιμετώπισης της τρομοκρατίας και των υβριδικών απειλών. Στο Σ. Μπλαβούκος, Δ.

Μπουραντώνης, & Π. Τσάκωνας (Επιμ.), Εξωτερικές σχέσεις της ΕΕ (σσ. 377–400). Εκδόσεις Ι. Σιδέρης.
25. Pawlak P. (2017, March). Countering hybrid threats: EU-NATO cooperation. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf
26. North Atlantic Treaty Organization. (2023, January 10). NATO and European Union leadership sign third joint declaration. https://www.nato.int/en/news-and-events/articles/news/2023/01/10/nato-and-european-union-leadership-sign-third-joint-declaration
27. Caliskan, Murat. (2019). Hybrid Warfare through the Lens of Strategic Theory. Defense and Security Analysis. 35. 40-58. 10.1080/14751798.2019.1565364.".
28. Λιαρόπουλος, Α. (2025). Το NATO απέναντι στην πρόκληση του Υβριδικού Πολέμου. Στο Α. Η. Μποζίνης, Α. Ν. Λιαρόπουλος, & Ι. Λ. Κωνσταντόπουλος (Επιμ.), Υβριδικές και αναδυόμενες απειλές στις διεθνείς σχέσεις (σσ. 17–44). Εκδόσεις Παπαζήση.
29. Rusinaitė, V. (2025). Turning strategy into praxis: Lessons in hybrid threat deterrence (Hybrid CoE Paper 25). European Centre of Excellence for Countering Hybrid Threats. https://www.hybridcoe.fi/wp-content/uploads/2025/08/Hybrid-CoE-Paper-25-Turning-strategy-into-praxis-web.pdf
30. Bajarūnas, E. (2025, 11 Φεβρουαρίου). Using NATO's Article 5 Against Hybrid Attacks. Center for European Policy Analysis. https://cepa.org/article/using-natos-article-5-against-hybrid-attacks/
31. Briant, E. L. (2015). Propaganda and counter-terrorism: Strategies for global change. Manchester University Press. https://research.monash.edu/en/publications/propaganda-and-counter-terrorism-strategies-for-global-change/