ANALYSIS

Mikhail Polianskii
December 2025

Getting out of the grey zone:

towards more European strategic clarity against Russian hybrid threats

Friedrich Ebert Stiftung

Imprint

Published by
Friedrich-Ebert-Stiftung e.V.
Godesberger Allee 149
53175 Bonn
Germany
https://www.russia.fes.de
info.russia@fes.de

Editing Department
International Cooperation Department,
Russia Program of the FES

Responsibility for content and editing
Alexey Yusupov

Photo credits
Cover: Illustrations Freepik.com, Pixabay.com

November 2025

Further information on this topic can be found here:
↗ https://www.fes.de/publikationen

Friedrich Ebert Stiftung

Mikhail Polianskii
December 2025

Getting out of the grey zone:

towards more European strategic clarity against Russian hybrid threats

Contents

Getting out of the grey zone:

towards more European strategic clarity against Russian hybrid threats

Europe faces an unprecedented escalation of malicious activities, frequently attributed to Russian state and non-state actors.[1] These activities blur the traditional boundaries between peace and war. In Germany alone, the Federal Criminal Police Office (BKA) reported 131,391 domestic cybercrimes and an additional 201,877 offenses originating abroad in 2024.[2] The digital association Bitkom estimates the annual loss to German companies from this source at 178.6 billion euros (€).[3] "Hybrid warfare" has become the dominant shorthand term for a wide spectrum of threats directed at Germany and its European allies,[4] ranging from the aforementioned cyber-attacks to incendiary devices planted in cargo planes and the sabotage of undersea cables.[5] But the very ubiquity of this term, debated in academic circles for nearly two decades and now increasingly adopted in policy discourse, introduces an added layer of ambiguity.

As Russian-sponsored malicious activities intensify across the continent, European leaders face an urgent dilemma, namely, how to categorise these threats adequately and craft effective responses, but without compromising the democratic values and stability they seek to defend. The present analysis examines these conceptual and practical challenges in terms of three critical foci: definitional precision, escalation dynamics and safeguarding democracy. Taken together, the following policy recommendations set out how Europe can more strategically navigate the grey zone between peace and open conflict, preserving both its security and its democracy.

First, the analysis demonstrates how terminological precision directly impacts policy effectiveness. When every cyber-attack, disinformation campaign or act of economic coercion is categorised under the broad umbrella of "hybrid warfare", analytical utility is diminished and resources risk misallocation.[6] By contrast, this analysis suggests a more nuanced approach that I label "analytical federalism". This recognises distinctive subcategories of attacks across the cyber, information, physical and other domains that merit individual treatment and response. Such a framework would prove useful in tailoring countermeasures to specific threats while streamlining coordination among defence, intelligence and diplomatic actors.

Second, it is argued that European decision-makers should be extremely careful in invoking war-related terminology in addressing hybrid threats because of its profound political and escalatory implications. While some European leaders argue that Russia's increasing hybrid attacks in Europe already amount to a de facto state of war, most prefer to characterise the current state of affairs as a "grey zone" between peace and open conflict.[7] The present analysis discusses the political repercussions of such terminological choices, elaborating how they can directly affect escalation dynamics, collective defence mechanisms and alliance cohesion.

Third, the final argument of this analysis is connected to Europe's practical responses to hybrid threats and their effects on the very democratic values it seeks to protect. Heavy-handed countermeasures – including media restrictions, expanded surveillance or punitive legislation – while seeming to make sense as an immediate response, may erode civil liberties and play directly into Moscow's strategic objectives in the long term. If such measures became mainstream, it would represent a victory for Russian hybrid warfare and so this must be avoided by strengthening fact-checking, political education and building up societal resilience through greater civic engagement.

These three dimensions are fundamentally interconnected: definitional precision enables appropriate responses, appropriate responses avoid unnecessary escalation, and avoiding escalation preserves space for democratic governance. Together, they contribute to a more coherent European strategy in an era of persistent grey-zone conflict.

1 Juraj Majcin (2025): Russia's threat to Europe goes beyond the battlefields of Ukraine, European Policy Centre, 2025; available at: https://www.epc.eu/publication/Russias-threat-to-Europe-goes-beyond-the-battlefields-of-Ukraine-6101fc

2 Bundeslagebild Cybercrime (2024): BKA setzt anhaltend hoher Cyberbedrohung zahlreiche Ermittlungserfolge entgegen. BKA; available at: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html

3 Bitkom (2024): Wirtschaftsschutz; available at: https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz.

4 Der Deutsche Bundestag (2025) Neues Lagebild zu hybriden Bedrohungen, 2025; available at: https://www.bundestag.de/presse/hib/kurzmeldungen-1103890?utm_source=substack&utm_medium=email

5 Cf. NATO (2024): Countering hybrid threats, 7 May; available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

6 Cf. Dan G. Cox, Thomas Bruscino and Alex Ryan (2012): Why hybrid warfare is tactics not strategy, *Military Strategy Magazine*, 4 April; available at: https://www.militarystrategymagazine.com/article/why-hybrid-warfare-is-tactics-not-strategy

7 Cf. Andre Bodeman (2025): Deutschland schon lange nicht mehr im Frieden, BR24; available at: https://www.br.de/nachrichten/deutschland-welt/general-leutnant-deutschland-schon-lange-nicht-mehr-im-frieden,Ua8q55u

Definitional precision: when everything becomes "hybrid"

Over recent years European security discourse has come to regard the term "hybrid warfare" as self-explanatory. But such widespread adoption has created a paradox: few actors agree on what the term really implies, and fewer still can explain how different interpretations of this phenomenon should shape different responses.[8] This conceptual inflation has generated practical challenges for policymakers, who struggle to distinguish between fundamentally different types of threat requiring distinct response mechanisms.

Consider the institutional confusion that the current definitional plurality creates for European states. NATO characterises hybrid warfare as "military and non-military, as well as covert and overt means (including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use of regular forces) to blur the lines between war and peace and destabilise and undermine societies".[9] The EU, by contrast, has adopted a broader approach, defining hybrid threats as "coordinated harmful activities that are planned and carried out with malign intent".[10]

These definitional differences reflect deeper intellectual debates within hybrid warfare scholarship that have been raging for several years. NATO's understanding aligns more closely with that of Frank Hoffman, the concept's founding father and a former US Marine, whose seminal 2007 study described hybrid warfare as "a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts and criminal disorder", all coordinated for synergistic effect.[11] European policymakers, on the other hand, tend to adopt definitions that resemble those found in the writings of contemporary scholars who emphasise that hybrid threats can encompass virtually any political activity that can be securitised.[12]

This divergence with regard to academic foundations helps to explain why NATO focuses on military-political thresholds (war vs peace), while EU approaches emphasise whole-of-society coordination and resilience. In short, the institutional confusion is not merely bureaucratic, but stems from fundamentally different scholarly traditions underlying use of the term "hybrid warfare". This divergence often results in obscuring the situation even more, instead of clarifying it. Consequently, the proliferation of this term in political debates about the "Russian hybrid threat" has led to what has occasionally been described as "categorical confusion", in which policymakers believe they are speaking the same language when in fact their words have different implications.[13]

Consider how even the closest European allies publicly talk past each other while discussing the current Russian hybrid threats. France's Chief of the Defence Staff Thierry Burkhard highlights that "NATO, which is a defensive military alliance that thinks in terms of peacetime and wartime", lacks tools "designed for the grey zone of competition and contestation". Interviewed for the same Politico article, former German intelligence chief Thomas Haldenwang emphasises the need to devise effective responses to Russia's "toolbox [of hybrid attacks], from influencing political discussions to cyber-attacks on critical infrastructure to sabotage on a significant scale".[14] Asked to describe the same phenomenon, these officials in fact stress entirely different aspects, clarifying the ambiguity of the grey zone (war vs peace) in contrast to countering the entire breadth of hybrid attacks. This case demonstrates that without centralised strategic dialogue on hybrid threats among key European powers, they are likely to continue to adopt divergent policy priorities that Russia can successfully exploit.

The precision problem becomes particularly acute when every incident is broadly labelled "hybrid warfare", regardless of its specific characteristics.[15] When analysts classify disinformation campaigns, physical sabotage and cyber intrusions within a single framework without further nuance, decision-makers lose sight of the specific vulnerabilities each exploits and the distinct countermeasures each requires. For instance, cyberattacks on critical infrastructure demand technical defensive measures, international cooperation on attribution, and potentially offensive cyber responses.[16] Disinformation campaigns, on the other hand, require strategic communications, media literacy programmes and targeted sanctions on propaganda networks. Finally, physical sabotage calls for enhanced security measures, intelligence cooperation and traditional law enforcement responses. In other words, each threat vector possesses distinct characteristics, exploits different vulnerabilities and responds to specific countermeasures.

8 Cf. James Wither (2023): Hybrid Warfare Revisited: A Battle of ›Buzzwords‹, *Connections QJ*, 22(1), pp. 7–27; available at: doi: 10.11610/Connections.22.1.02.

9 Cf. NATO (2024): Countering hybrid threats, 7 May; available at: https://www.nato.int/cps/en/natohq/topics_156338.htm

10 European Council (2025): Hybrid threats; available at: https://www.consilium.europa.eu/en/policies/hybrid-threats

11 Frank G. Hoffman (2007): Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies.

12 Cf. Andrew Mumford, and Pascal Carlucci (2023): Hybrid warfare: The continuation of ambiguity by other means, *European Journal of International Security*, 8(2), pp. 192–206; available at: doi: 10.1017/EIS.2022.19.

13 Cf. Colin S. Gray (2020): Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional, Strategic Studies Institute Monograph, US Army War College; available at: https://press.armywarcollege.edu/monographs/561

14 Both quoted in: Laura Kayali (2024): Europe is under attack from Russia. Why isn't it fighting back?, Politico, 25 November; available at: https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference

15 Cf. Alina Bârgăoanu and Elena Negrea-Busuioc (2024): Hybrid warfare is less than warfare: a dangerous illusion, Irregular Warfare Center; available at: https://irregularwarfarecenter.org/wp-content/uploads/P_19_Hybrid_Warfare_is_Less_Than_Warfare.pdf

16 Mikhail Polianskii (2025): Digitale Zeitenwende: Aktive Cyberabwehr als Antwort auf Russlands hybride Kriegsführung, PRIF-Spotlight 6; available at: https://blog.prif.org/en/2025/07/16/digitale-zeitenwende-aktive-cyberabwehr-als-antwort-auf-russlands-hybride-kriegsfuehrung

When these distinctions become obscured under a catch-all "hybrid warfare" label, resources are misallocated, responses become generic rather than targeted, and coordination suffers because agencies lack clear guidance about their specific roles.

The practical solution should not be to abandon the hybrid warfare concept altogether (as some analysts have suggested). Instead, policymakers and analysts should consider adopting an analytical "federalism" approach, maintaining hybrid warfare as a strategic umbrella term, while creating precise subcategories for operational planning. This would help European policymakers to better navigate between disparate cyber hybrid threats (requiring technical responses), information hybrid threats (requiring communications responses), and kinetic hybrid threats (requiring conventional security responses).

In sum, the term "hybrid warfare" is problematic and likely to remain so for decades to come. Nevertheless, its widespread proliferation demonstrates that it responds to a genuine analytical need in describing current attacks on European soil from countries such as Russia. Adopting a more streamlined and unified definition at the meta-level through strategic dialogue while deepening analytical precision at the operational level may prove instrumental in developing more effective policy formulation and resource allocation. This approach would enable practitioners to understand how individual attacks fit into broader strategies, while responding appropriately to each attack's specific characteristics. Such an analytical foundation becomes even more essential when considering the escalation dynamics that terminological choices can trigger, which is the focus of the next section.

Rhetorical choices and their consequences: the political costs of "war" terminology

The EBU Investigative Journalism Network has documented hundreds of confirmed or suspected cases of Russian activities against Europe since 2022, ranging from incendiary devices in DHL cargo planes "strong enough to have brought down a cargo plane" to severed undersea cables disrupting Baltic communications,[17] GPS spoofing in the Baltic region affecting civilian aviation, and sophisticated cyberattacks on critical infrastructure.[18] While individually these attacks might appear to be relatively contained, their significant cumulative impact raises a fundamental question: do these acts, taken together, constitute de facto undeclared war?[19]

How European leaders answer this question has profound implications that extend far beyond semantic preferences.[20] The choice to invoke – or avoid – "war" terminology can directly affect escalation dynamics, collective defence mechanisms, domestic political support and alliance cohesion, all of which policymakers must navigate carefully.

The political costs of imprecise war rhetoric became particularly evident in the controversy surrounding former German Foreign Minister Annalena Baerbock's statement that *"we are fighting a war against Russia"* during a Council of Europe meeting. The German government immediately faced pressure to clarify that Baerbock meant supporting Ukraine's defence rather than declaring direct war, after criticism that her statement could be interpreted to imply that Germany had become a war party.[21]

This incident illustrates how war terminology can create strategic confusion when words fail to align with actual policy positions. This may undermine both domestic credibility and international coordination. When individual European leaders embrace war rhetoric while NATO simultaneously maintains that it "is not at war with Russia", the resulting dissonance breeds confusion among allies and provides Russia with propaganda opportunities.[22] Moscow's propaganda systematically exploits this confusion by amplifying aggressive Western statements to justify escalation while dismissing moderate positions as evidence of Europe's weakness.[23]

The risks of misusing war terminology, however, extend far beyond propaganda battles; they can affect real policy choices. When European media and policymakers constantly invoke "war" by adding "hybrid" to it and call for retribution,[24] dangerous feedback loops can develop in which each side claims that the other has crossed a war threshold. This dynamic can lead to escalation-counter-escalation cycles, significantly heightening the risk of a miscalculation that could trigger real military confrontation. As Daniel Byman of CSIS observes, European leaders should exercise extreme caution when discussing ways of carrying on a "hybrid war" against Russia because otherwise they might be "drawn into a conflict [with Russia] for which they're not prepared".[25]

Collective defence mechanisms add an additional layer of complexity for European NATO members. The alliance

17 CNN (2024): Baltic Sea internet cables cut: European officials cry sabotage, 19 November; available at: https://www.cnn.com/2024/11/18/europe/undersea-cable-disrupted-germany-finland-intl

18 EBU Investigative Journalism Network (2025): Playing with fire: EBU investigates Russia's hybrid attacks on Europe, 12 March; available at: https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war

19 Cf. Center for Strategic and International Studies (CSIS) (2025): Russia's Shadow War Against the West, 18 March; available at: https://www.csis.org/analysis/russias-shadow-war-against-west

20 Cf. Lawrence Freedman (2023): The Language of War; available at: https://samf.substack.com/p/the-language-of-war

21 Deutsche Welle (2023): Germany says it is not a warring party in Ukraine, 27 January; available at: https://www.dw.com/en/germany-says-it-is-not-a-warring-party-in-ukraine/a-64541484

22 NATO (2024): Setting the record straight: de-bunking Russian disinformation on NATO, NATO HQ; available at: https://www.nato.int/cps/en/natohq/115204.htm

23 Cf. Sergey Lavrov (2025): Virtually all of Europe is at war against Russia, TASS; available at: https://tass.ru/politika/23862257

24 Europe is under attack from Russia. Why isn't it fighting back?, Politico, 25 November 2024; available at: https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference

25 Ibid.

stated during the Vilnius summit in 2023 that "hybrid operations against Allies could reach the level of an armed attack and could lead the Council to invoke Article 5 of the Washington Treaty".[26] However, Article 5 famously remains ambiguous, specifying only "actions that allies [deem] necessary", which can mean very different things.[27] While strategic ambiguity serves important purposes[28] – maintaining uncertainty about response thresholds can complicate Russian operational planning on different levels – Russian behaviour observed thus far suggests that Moscow is not particularly deterred by this uncertainty. The Kremlin recognises that there are no automatic mechanisms when it comes to triggering Article 5 in instances of hybrid attack and thus far it has successfully tested boundaries below defined thresholds, exposing NATO gaps in the existing deterrence mechanisms.[29]

In this vein, some critics in policymaking circles argue that current "hybrid war" terminology does not go far enough in deterring Russian attacks. The former Lithuanian Foreign Minister Gabrielius Landsbergis, for instance, contended that: "When Russia is involved in direct kinetic attacks, we should find another name to call it. I would prefer to call it a terrorist attack, state-sponsored terrorist attack."[30] Danish Prime Minister Mette Frederiksen similarly argues, "We are simply too polite [by calling it hybrid]".[31] They believe that euphemistic language involving "hybrid" obscures the gravity of the situation and allows Russia to continue its aggression without fearing robust responses.

The path forward requires striking a balance between deliberate ambiguity about ultimate responses and clear, graduated actions to specific types of hybrid attack. By developing precise countermeasures within the suggested "analytical federalism" framework – specific and symmetric responses for cyber, information, economic and kinetic hybrid threats – European leaders can enhance collective deterrence without being sucked in to increasing escalation with Russia. Such a balanced approach would provide the strategic flexibility necessary to effectively counter Russian hybrid aggression at every level, while preserving the democratic constraints that such responses must respect. This topic is analysed in the penultimate section.

Practical responses and democratic constraints: safeguarding governance while countering threats

Europe's confrontation with Russian hybrid threats creates a fundamental dilemma: how to develop robust defences without compromising the freedoms and principles that make democratic societies worth defending. This challenge is particularly acute because a primary objective of Russian hybrid campaigns is to undermine democratic norms, deliberately targeting public trust in institutions, press freedom and the rule of law.[32]

The temptation to adopt heavy-handed countermeasures might be understandable when democracies face sustained hybrid attacks. Disinformation campaigns prompt calls for expanded censorship, but they can also be repurposed to silence legitimate dissent.[33] Cyber threats must be tackled head on, but they might also be used as an excuse to justify enhanced surveillance capabilities that may infringe on privacy rights. Foreign influence operations create pressure for restrictions on civil society organisations, academic exchanges and international cooperation, which form the backbone of open societies.[34] Every defensive measure, while potentially beneficial for security in the short term, carries the long-term risk of transforming democratic societies into something resembling the authoritarian systems they oppose.

Such frequently emotional responses are part of the strategic trap that Moscow is aiming to spring. If European democracies respond to hybrid threats by becoming less democratic, they hand Russia a significant victory regardless of whether the original attacks succeed. Russian hybrid warfare aims not just to achieve immediate tactical objectives but to provoke overreactions that damage democratic institutions over time.

Poland's recent media restrictions illustrate this dynamic. The previous Law and Justice Party government's attempts to control public media and restrict foreign ownership of media companies sparked serious concerns about press freedom and democratic governance.[35] While proponents argued that such measures were necessary to counter foreign influence and disinformation – including from Russia – critics warned that they could be weaponised against

26 NATO Vilnius Summit Communiqué, 11 July 2023. Section 64; available at: https://www.nato.int/cps/en/natohq/official_texts_217320.htm

27 Eitvydas Bajarūnas (2025): Using NATO's Article 5 Against Hybrid Attacks, CEPA, 13 February; available at: https://cepa.org/article/using-natos-article-5-against-hybrid-attacks

28 Cf. War in Ukraine: Strategic Ambiguity finds renewed significancy in 21st-century Nuclear Deterrence, Le Monde; available at: https://www.lemonde.fr/en/opinion/article/2022/11/28/war-in-ukraine-strategic-ambiguity-finds-renewed-significance-in-21st-century-nuclear-deterrence_6005911_23.html

29 Cf. Viktorija Rusinaitė (2025): Turning strategy into praxis: Lessons in hybrid threat deterrence, Hybrid CoE; available at: https://www.hybridcoe.fi/publications/turning-strategy-into-praxis-lessons-in-hybrid-threat-deterrence

30 Lithuanian Ministry of Foreign Affairs (2024): Landsbergis at the NATO summit, 12 July; available at: https://www.urm.lt/en/news/928/landsbergis-at-the-nato-summit-a-very-strong-message-is-being-sent-to-moscow:42922

31 Quoted in »Europe is under attack from Russia. Why isn't it fighting back?«, see n 24 above.

32 Cf. Carol Atkinson (2018): Hybrid Warfare and Societal Resilience: Implications for Democratic Governance, Information & Security: An International Journal, 39(1), pp. 63–76; available at: doi: 10.11610/ISIJ.3906.

33 Jon Bateman and Dean Jackson (2024): Countering Disinformation Effectively: An Evidence-Based Policy Guide; available at: https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en&utm

34 Cf. The Civil Society State of Union 2024 – Report; available at: https://civilsocietyeurope.eu/wp-content/uploads/2023/09/CSE-State-of-the-Union-DIGITAL-accessible-in-progress.pdf

35 Reuters (2021): EU voices concern over Polish media bill, impact on press freedom; available at: https://www.reuters.com/business/media-telecom/eu-voices-concern-over-polish-media-bill-impact-press-freedom-2021-12-20

domestic political opponents, too.[36] Powers granted ostensibly to counter hybrid threats did not remain limited to their original purposes and were taken up as tools of partisan political control that may undermine democratic accountability.

The European Union's Digital Services Act presents similar challenges on a continental scale. While designed to combat disinformation and foreign manipulation, the legislation grants platforms and regulators broad authority to remove content deemed harmful or misleading.[37] Critics warn that this might "set the stage for widespread censorship, curtailing lawful and truthful speech under the guise of compliance and safety".[38] The balancing act, however, consists of distinguishing between foreign manipulation campaigns and legitimate political discourse. This task becomes increasingly difficult in polarised societies, in which inconvenient information may be dismissed as "disinformation".[39]

These and similar reactive countermeasures provide Moscow with exactly the propaganda ammunition it seeks. Russian propaganda systematically exploits Western restrictions on speech and media as evidence that democratic values are merely a facade. Russian outlets regularly highlight European measures against RT, Sputnik and others, arguing that such social media content moderation and expansion of surveillance are hypocritical and ultimately no different from authoritarian governance.[40] While there is no justification for Russia's propaganda activities, it is worth mentioning that attempting to impose outright bans on Russian and other outlets may turn out to be like fighting the proverbial hydra, while potentially alienating domestic populations who value civil liberties.

Moving forward requires targeted, proportionate responses that strengthen rather than weaken democratic institutions. This demands careful design of counter-hybrid policies with strict limitations and oversight mechanisms, combined with transparent communication about their necessity, scope and limitations. Rather than restricting democratic space, effective responses should expand it, enhancing media literacy, strengthening fact-checking capabilities and building up societal resilience through enhanced civic engagement.

By responding to attacks on democracy with more democracy, Europe can deny Moscow both its immediate tactical objectives and its broader strategic goal of undermining democratic legitimacy. The problem lies in maintaining the moral and political authority that comes from practicing the values Europe seeks to defend, ensuring that defensive measures enhance rather than compromise democratic institutions.

Conclusion

The three dimensions examined in this analysis are fundamentally interconnected, forming a coherent framework for European strategy in the era of "grey-zone" conflict. Terminological precision enables appropriate responses by clarifying what different threats require, based on what I call "analytical federalism". Appropriate responses help to avoid unnecessary escalation by matching means to ends and preserving alliance cohesion. Avoiding escalation preserves space for democratic governance by preventing crisis-driven authoritarianism that would serve Moscow's strategic objectives.

This interconnection demands that European strategy be holistic rather than compartmentalised. Policymakers cannot address definitional questions in isolation from escalation concerns, nor can they build resilience without considering democratic constraints. The "analytical federalism" framework offers a practical path forward, maintaining hybrid warfare as a strategic integration concept while developing precise subcategories for operational responses. This approach enables targeted countermeasures that address specific vulnerabilities at the operational level without triggering unnecessary escalation or compromising democratic values.

Clear concepts enable clear choices, and clear choices enable effective strategy. In an era of grey zone conflict in which conceptual confusion serves primarily those who seek to undermine democratic governance and European security, achieving such clarity represents both an analytical imperative and a strategic necessity. The stakes extend far beyond academic debate to encompass the fundamental question of how democratic societies adapt to new forms of conflict while preserving their essential character.

36 Agata Pyka (2025): Resisting foreign interference: Poland's presidential election and the Russian challenge, New Eastern Europe; available at: https://neweasterneurope.eu/2025/06/10/resisting-foreign-interference-polands-presidential-election-and-the-russian-challenge/#:~:text=Based%20on%20those%20measures%2C%20Poland,if%20necessary%2C%20take%20it%20down

37 European Commission, Digital Services Act, 2022; available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

38 Adina Portaru (2025): Unpacking the EU Digital Services Act, ADF International, 28 January; available at: https://adfinternational.org/commentary/eu-digital-services-act-one-year#:~:text=The%20EU%20Digital%20Services%20Act's,principles%20it%20claims%20to%20protect

39 Ibid.

40 The EU's "Ban" on RT and Sputnik: A Lawful Measure against Propaganda for War, Verfassungsblog, 8 March 2022; available at: https://verfassungsblog.de/the-eus-ban-of-rt-and-sputnik

About the author

Dr **Mikhail Polianskii** is a postdoctoral researcher at the Peace Research Institute Frankfurt (PRIF), focusing on Russian foreign policy, European security, and hybrid warfare. He completed his PhD at Goethe University Frankfurt in 2024 with a dissertation titled “Better Shared Than Dead? Russia’s Dissociation from the Post-Cold War European Security Order.” He is currently working on the research project “PATTERN: How Does the Past Matter? The Russian War of Aggression Against Ukraine and the Cold War”, which analyses whether – and how – the lessons of the Cold War can help transform today’s confrontation with Russia and other antagonistic great powers into more regulated forms of deterrence, coexistence, or cooperation.

Getting out of the grey zone:

towards more European strategic clarity against Russian hybrid threats

→

Europe faces an intensifying campaign of cyber, informational and physical operations by Russian state and non-state actors designed to blur the boundary between peace and war. "Hybrid warfare" has become the shorthand for this spectrum of threats, but its indiscriminate use breeds analytical vagueness and policy overreach.

→

This analysis argues that strategic effectiveness begins with conceptual clarity. It advances an **"analytical federalism"** that disaggregates hybrid activity into distinct cyber, information, economic and kinetic subdomains, allowing for tailored counter-measures and more coherent coordination across institutions. It also warns that uncritical war rhetoric risks fueling escalation, fracturing alliance cohesion and closing off diplomatic options.

→

Finally, it cautions that defensive overreach – through media restrictions or expanded surveillance – may erode the very democratic norms Europe seeks to protect. By linking definitional precision to calibrated responses and democratic resilience, the analysis offers policymakers a roadmap for navigating the grey zone without sacrificing either security or liberal values.

Further information on this topic can be found here:
↗ **www.fes.de**

Friedrich Ebert Stiftung