ISSUE 01 SEPTEMBER 2026

THE NEXT GENERATION OF STRATEGIC THOUGHT

SSI Youth Voices

A NOTE FROM THE FOUNDER

Strategic thinking should not belong only to those who already hold positions of power. The security environment is changing rapidly, and the decisions being made today will shape the world in which the next generation will live and lead. Young people are not simply observers of these changes. They are already part of the conversation, bringing new perspectives, questioning established assumptions, and thinking about security beyond traditional boundaries.

SSI Youth Voices was created to provide a space for that thinking. At the Strategic Security Initiative, we believe that meaningful policy discussions benefit from diverse perspectives and that young researchers and emerging professionals should have opportunities to develop, challenge, and share their ideas. This publication is one way of creating that space.

The first issue, "The Next Generation of Strategic Thought," brings together young voices reflecting on the questions that are shaping international security and strategic affairs. Some of these perspectives may challenge conventional thinking. That is precisely the point.

This is not intended to be a publication that simply reproduces established narratives. It is an invitation to think critically, ask difficult questions, and imagine what strategic thinking should look like in the years ahead.

I hope SSI Youth Voices becomes not only a publication, but a growing community of young people who are willing to engage seriously with the complexities of our time.

MEGI BENIA

Founding Director
Strategic Security Initiative (SSI)

EDITORIAL TEAM

This issue was edited by Salome Nadashvili, Senior Editor of SSI and Megi Benia, Founding Director of SSI

Photo: Yevgeny Prigozhin, and fighters in Bakhmut, May 20, 2023. AFP

Ana Kakulia

Remaining Below the Threshold of State Responsibility: Russia's Use of the Wagner Group in Bakhmut

The War in Ukraine fundamentally changed the international landscape, altering perceptions of how warfare is conducted and creating an environment in which the operational patterns and rules of engagement of forces are difficult to discern. In these volatile conditions, Russian methods for engaging in conflict have shifted, or rather, evolved to fit the demands of the modern understanding of war. This policy Paper explores one such method: employing proxy forces, in this case, the Wagner Group, to achieve the specific objective of staying below the threshold of state responsibility.

In modern times, the most concerning threat is one that cannot be accurately identified, categorized, and assessed. The ambiguous nature of the Wagner Group and its elusive ties to the state during its operations in Bakhmut foster uncertainty. Russia has historically employed the military deception strategy of Maskirovka. In light of this legacy, utilizing Wagner becomes even more concerning. Hence, the purpose of this work is to thoroughly analyze the actions of Russia and the group, with the aim of formulating a more comprehensive idea of how these operations were carried out and preventing hostile actors from exploiting structural deficiencies for their benefit.

The Wagner Group Misnomer

Though colloquially referred to as a Private Military Company (PMC), for Wagner, the title is not definitionally applicable. PMCs are understood as private, profit-maximizing entities, often hired by governments "to kill or train others to kill"[i]. The key divergence from the Western interpretation lies in the word "private." The scope of governmental involvement in the internal operations of these firms is supposed to be limited – this cannot be said about Wagner and the state. Its deep links to the Russian Military Intelligence Service (GRU) and the Ministry of Defense have led many experts to label it as a "GRU-controlled special force".[ii] The Russian discourse on the topic adds to the confusion. Having not yet been officially recognized or regulated, Russian spokespeople have followed the model of denial and distancing. Simply put: as there is no law in Russia on PMCs, they do not exist, nor do they fall under the authority of the state.[iii]

There are no official legal clauses on PMCs in Russia. However, Article 359 of the Criminal Code does prohibit mercenarism. The document defines a mercenary as "a person who acts for the purpose of getting a material reward, and who is not a citizen of the state in whose armed conflict or hostilities he participates, who does not reside permanently on its territory, and also who is not a person fulfilling official duties"[iv]. This conceptual limitation directly discredits the validity of the Wagner recruits being considered mercenaries.

The most comprehensive understanding of Wagner comes from Kimberly Marten, who calls Wagner a "semi-state informal security organization",[v] being partially recognized, apparently illegal, and with an opaque relationship to the Russian state. Rondeaux similarly uses a more complex term, referring to Wagner as an "irregular Paramilitary Contingent".[vi] Though neither fully developed nor established, both of these concepts are much more in tune with the true essence of Prigozhin's forces. The confusing, underexplored, and deliberately ambiguous nature of Wagner undoubtedly makes the process of attribution more difficult.

The war in Ukraine and Wagner in Bakhmut

Russia began its full-scale invasion of Ukraine in February of 2022, attacking with approximately 200,000 troops from Crimea in the south, Belarus in the north, as well as from its own territory in the east. Though unprovoked, the hostilities had been rising

for years.[vii] Originally, Bakhmut was not a significant military objective. It was supposed to serve as a stepping stone for Russia to secure the city of Slovyansk and encircle the Ukrainian forces in the east. This would enable the state to take control of the administrative borders of the Donetsk Oblast. As the Russian advances failed, by March-April of 2023, the battle for Bakhmut became strategically obsolete. Despite the absence of operational importance, the fighting persisted largely due to its symbolic significance.[viii]

Throughout the war, the Wagner forces have been implicated in several acts of violence against the civilian population, such as targeting civilian children, tossing grenades into ditches holding captive Ukrainian soldiers and deserters,[ix] as well as several instances of mistreatment of Ukrainian prisoners of war.[x] The human rights abuses were carried out against the group members as well, by other operatives.[xi] In the case of Savichev and Uldarov, two ex-Wagner members who admitted to killings were threatened with the combined forces of Russian federal authorities and Wagner forces. It seems that committing crimes is permissible, though speaking out will lead to being punished.[xii]

The recruitment process for Wagner, known as "Project K", included enlisting prisoners from the Russian penitentiary system.[xiii] The Group's enlistment strategy was state-sanctioned or at least state-approved. Prigozhin's phone records and calendar entries reveal that the Wagner chief had established contact with federal prison officials beforehand, with numerous meetings with FSIN officials.[xiv]

The structure of the Wagner Group in Bakhmut can be described as disjointed, serving as a "separate unit" that was a part of the Russian Troops and often deployed on the front lines, treated as disposable.[xv] This fits into the framework of Wagner having "operational independence".[xvi] Though at some points during the battle, the opposite was true, with a Ukrainian Colonel stating that as of April 24, the Wagner Group was no longer able to conduct operations without Russian Airborne and special-purpose units' support,[xvii] pointing to the dependence of the group on the official Russian military formations.

Throughout the battle, Prigozhin criticized Russian bureaucracy and officials for not providing sufficient support, as well as blaming them for the disproportionately high losses suffered by Wagner. Additionally, Prigozhin unilaterally and seemingly without premeditated coordination with the Russian state declared that the Wagner forces had

taken Bakhmut.[xviii] Though the verbal confrontation was seemingly resolved with the president's statement, this example points to the lack of synchronization between the Russian state and the official Wagner leadership. In response to the fall of Bakhmut, the state media was in a 20-hour media blackout.[xix]

The final aspect to consider is that of Prigozhin's dissatisfaction with the Russian Ministry of Defense, which made the Wagner chief more of a liability than an asset for Putin. One such attempt at curbing Prigozhin's platform came to light when a Wagner-affiliated media channel published a leaked document issued by the Russian state, which gave a directive to stop mentioning Wagner or Prigozhin, the existence of which was denied[xx]. Apart from the media involvement, the division between Wagner and the state also presented itself on a structural level, having been identified as a possible factor behind the replacement of high-ranking Russian officials like Sergey Surovkin.[xxi]

Remaining Below the Threshold of State Responsibility

To create an effective framework for evaluating the group's actions, the term "staying below the threshold of state responsibility" is understood as the synthesis of the security studies concept of staying below the threshold of armed conflict and the international law understanding of state responsibility. To create a conceptual link, the threshold of armed conflict can be measured through the scale and typology of measures, while the conceptual line for state responsibility is drawn at attributability and the level of effective control over an entity. Based on the preexisting concepts, the policy paper identifies four assessment criteria to evaluate whether Russia has employed Wagner to remain below the threshold of state responsibility:

- *Ambiguity*: The term is used to describe any activity that is deliberately confusing or underexplained, to make attribution of an action to a specific actor difficult.
- *plausible deniability*: This concept denotes the denial or the lack of accountability for a certain activity based on a lack of knowledge. This tactic is carried out either by outright denial from officials or through the employment of media channels that influence the narrative.
- *Coercive Gradualism*: The paper modifies the term to also include incremental, gradual change in activity that has the primary or secondary goal of avoiding the direct triggering of state responsibility. While the core method remains the same, the purpose is understood differently.

- *Multifaceted Approach*: In this context, the approach implies the synchronized, simultaneous use of various tactics of all natures, ranging from material to rhetorical, with the end goal of reaching a certain objective, in this instance, the avoidance of state responsibility.

Avoidance of Responsibility Through the Use of Ambiguity

As it has already been established, the absence of concrete definitions and frameworks makes the process of attribution difficult. The term PMC fails to encompass the unique characteristics of the group, while the concepts of a mercenary organization or a state organ are not definitionally applicable. The lack of regulatory and explanatory tools can be interpreted as the first example of the deliberate fabrication of ambiguity by the state.

Similarly, the recruitment procedure for Wagner Group members for the battle has been shrouded in mystery. Though the FSIN connection to Russia is straightforward, the official state-Wagner relationship during the recruitment process remains non-linear and largely ambiguous, relying mostly on interpersonal connections and familiarity with the system. The lack of official documentation renders the process of identifying authority figures and the chain of command difficult. What entity or person would be responsible for monetarily compensating the prisoners or their families, and who would be their de jure employer?

When assessing the situation, Prigozhin's role and rhetoric must be considered. Prigozhin's relationship with the ruling elite had deteriorated, his speeches becoming increasingly aggressive and inflammatory. The Wagner leader's dissatisfaction with the Russian officials and the bureaucracy, coupled with his unilateral declaration of victory in Bakhmut, paints a picture of discord between Wagner and Russia. During the Battle, the leader clearly demonstrated his ambition to be viewed separately from the official Russian army contingent. Though Prigozhin may have fostered this division with different intentions, the end goal was that he inadvertently drew a line between Wagner and forces operating under direct Russian control.

Though the catalogue of violations is extensive, the specific details of these cases, as described, are either unverifiable, scarce, or completely absent. This once again highlights the difficulty in accurately tracing back and attributing actions to the Wagner Group. Consequently, the extent of state involvement and culpability also remains

unclear. The internal makeup of Wagner and the multiple recorded clashes with official arms call into question Russian control over the entity. There exists no single consistent structure for how the Group operates, whether it acts independently or is reliant on the support of the state for combat.[xxii] The structurally fragmented and inconsistent nature of the entity makes the process of finding an "organic link"[xxiii] with the state difficult. Herein lies the essence of ambiguity – Russia has blurred its connection to the Wagner Group to such an extent that no straightforward nexus can be identified.

The Utilization of plausible deniability

plausible deniability is complementary to the concept of ambiguity, especially in reference to the Russia-Wagner connection. The vague ties between the state and the entity allow it to claim plausible deniability over the war crimes committed by operatives in Bakhmut. The specific case of the Saratov Oblast Investigative Committee's arrest of former Wagner members presents a clear picture of state distancing. By making the arrest, the federal authority, despite working with the Wagner Group, indirectly denounced the war crimes of Uldarov and Savichev, drawing a symbolic line between the state and the group. The hypothesis that Russia attempted to preserve plausible deniability is strengthened when we consider how the dissident voices of former operatives were suppressed and why deserters were punished. The argument would be that former members who could shed light on Wagner-state interconnectedness were intimidated or indoctrinated into silence.

When assessing the actions of the state through the lens of plausible deniability, one must consider the example of the unofficial Russian edict that limited coverage of the Wagner Group. The Russian channels did not cover the issue for 20 consecutive hours. This information is extremely pertinent, as Russian state-controlled and supporting media have been historically and actively employing the model of propaganda often described as "the firehose of falsehood". State-supporting sources propagate large volumes of repetitive and confusing information through multiple channels, with a lack of regard for objective truths, with the end goal of disorienting and overwhelming the audience[xxiv]. Alas, the tried-and-tested model of Russian propaganda was noticeably absent for the 20 hours following Prigozhin's statement. The lack of credibility of the information would not have been a deterrent, so the Wagner chiefs' argument that the Russian media deliberately omitted coverage of the situation in Bakhmut might have

contained an element of truth. It can be deduced that the Russian state had utilized its influence on the media apparatus to limit coverage of Wagner when it went against the objectives of the state, avoiding the amplification of statements that could either implicate Putin or paint him in an unfavorable light. This model of distancing became the precursor to eventually bringing the "irregular paramilitary contingent" fully under Russian control.[xxv] The tactic of either amplifying or, in this case, silencing certain topics is a clear attempt by the Russian state to control the narrative and create a safeguard against implication.

The Strategic Employment of Coercive Gradualism

Coercive gradualism can be identified in the timeline of Russia's employment of the Wagner Group: the measured rise in prisoner recruits and localized, at times, minimal use of the forces all point to gradual escalation. The ebb and flow of the group's involvement seems calculated, though not fully controllable; a strategy of slow integration takes shape. Furthermore, the gradual tonal shift in the rhetoric of Russian officials also needs to be considered. It can be described, though cautiously, as a premeditated response with the ultimate goal of normalizing Wagner's involvement.

The escalation of using prisoner recruits as "cannon fodder" was also gradual, meaning the Russian strategy of avoiding culpability applied to Prigozhin's operatives themselves. The high expendability of the Wagner forces could have been explained, if not for the fact that the names and backgrounds of these persons have been procured by the BBC-Mediazona joint investigation. It could have been argued that their use as "cannon fodder" was permissible for the state, as the lack of evidence regarding their affiliation would have made the process of attribution more complex. However, as it stands, this is not the case. If the intent behind using Wagner operatives on the front lines was to avoid culpability through the lack of evidence, this approach was, in practice, unsuccessful. It is more likely that as the war effort progressed, it became apparent that the state could utilize the Wagner forces in this manner, without incurring the costs of admitting state responsibility.

Adopting a Multilayered Approach

The use of political rhetoric, deliberate lack of definition and regulation, the unconventional structure of the Wagner Group and its lack of official institutional separation or incorporation into the Russian forces, along with the unorthodox

recruitment process from federal prisons, when taken together, demonstrate the full extent of the Russian multilayered strategy.

The use of a multilayered approach is attractive, as no single method can guarantee success. For instance, if the Russian state lost control of the narrative due to the Wagner chief's unpredictable nature, it could rely on the utilization of the media apparatus to push its own agenda and avoid admitting responsibility. To exemplify further, if intimidation or the promise of financial compensation failed, Russia could rely on the employment of state organs or delegate the task of preserving secrecy to the Wagner chief himself, as shown with Uldarov and Savichev. Furthermore, preserving Plausible deniability was only made possible due to the intricate network of connections between the Russian Federation and the Wagner Group, in conjunction with the state's connection to the media apparatus.

Here, a complex, interlocked structure emerges, one that possesses varying components that are inextricably tied, often intersect, and serve to ensure the functionality of the whole system. The conclusion is twofold: First, the research asserts the existence of violations in Bakhmut and the subsequent Russian attempt at obfuscating responsibility. Second, it can be deduced that these actions were in no way isolated but a part of a calculated, multilayered model, designed to blur the lines of blame.

Recommendations

The recommendations have been categorized in order of feasibility for quick implementation, covering the conceptual, institutional and legal levels:

1. **Conceptual: Establishing a multidimensional understanding of proxy warfare** - Though proxy force activity is already envisaged as a possible aspect of hybrid warfare, the intricacies of its composition are not broadly understood. The policy paper sought to highlight how Russia has employed Wagner through an integrated strategy that was made up of four interconnected components. The overarching recommendation of the paper is for the international community to stop viewing this threat as homogeneous, but rather acknowledge that the fabricated ambiguous environment, the utilization of plausible deniability, the new tactic of incrementally increasing pressure and the means of coercion, and lastly,

the combination of all of these approaches must be envisaged as different components of a single Russian strategy, packaged in the format of proxy warfare.

2. **Institutional: Institutionalizing a dedicated autonomous body for proxy attribution and research** – NATO and the EU have a strong and well-established cooperative relationship. With regular exchanges between bodies such as NATO's Joint Intelligence and Security Division (JISD) and the EU's Single Intelligence Analysis Capacity (SIAC). The deficiency of this system is that it remains too broad; to combat this, the policy paper proposes a consulting body specifically dedicated to proxy force attribution and research built on the model of the European Centre of Excellence (Hybrid CoE), an autonomous think tank providing a platform for information-sharing on hybrid threats.[xxvi] To specify, it would be an autonomous, collaborative information-sharing and expertise body specifically dedicated to studying proxy forces in the context of hybrid warfare. The body would emphasize and continue the legacy of cooperation with affected countries, acting as the primary source. In the context of the use of proxy forces like Wagner, Ukraine would serve as the primary collaborator, building on the security coordination mechanism it already has with NATO.

3. **Legal: Enhancing the adaptability and specificity of the international law architecture for proxy forces like Wagner** - The international law texts, such as Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), could, in theory, apply to Wagner's activity in Bakhmut. However, the difficulty lies in establishing the effective control encoded in Article 8.[xxvii] There is no concrete documentation or admission from the state. To this end, the policy paper suggests a two-fold solution:

- Creating clear guidelines for establishing legal attribution, thereby specifying what effective control can entail, not changing the text but rather expanding on what the effective control concept can entail.
- Utilizing the research, knowledge, and evidence from the collaborative and autonomous information-sharing body, discussed in the second recommendation, to prove or discredit a state's liability for a proxy force's action in accordance with ARSIWA.

CONCLUSION

The policy paper has sought to evaluate the role the Wagner Group played in enabling Russia to remain below the threshold of state responsibility. Several key aspects were explored, specifically, the deep-seated connection between the entity and the state, the ambiguity within its command structure, its unusual operational style, and the lack of concrete understanding regarding the status of the group. The goal of the paper was to enrich the field of study on both the Wagner Group and the tactics employed by the Russian Federation to evade state responsibility.

Understanding the threat, how it operates, and how it can be accurately defined and assessed is vital for formulating an effective defense posture. Though PMC remains a misnomer for the true nature of the Wagner Group, McFate's description of such entities "that kill or train others to kill" can be modified to capture the broader goal of the paper: to enable states to defend and train others to defend.

Photo: Yevgeny Prigozhin talks to Wagner fighters in the course of Russia-Ukraine conflict in Bakhmut, Ukraine, May 25, 2023. Press service of "Concord"/Handout via Reuters

[i] S. McFate, *The Modern Mercenary: Private Armies and What They Mean for World Order* (Oxford University Press, 2014), 1, 9.
[ii] N. Dahlqvist, *Russia's (Not So) Private Military Companies*, FOI Memo 6653, RUFS Briefing no. 44 (Swedish Defense Research Agency, January 2019), 1, https://www.foi.se/rest-api/report/foi%20memo%206653.
[iii] K. P. Larsen, "From Mercenary to Legitimate Actor? Russian Discourses on Private Military Companies," *Post-Soviet Affairs* 39, no. 6 (2023): 13, https://doi.org/10.1080/1060586X.2023.2247782.
[iv] Criminal Code of the Russian Federation, *Criminal Code of the Russian Federation, Article 359: Mercenarism* (State Duma of the Russian Federation, 1996), art. 359, https://www.consultant.ru/document/cons_doc_LAW_10699/a9e28227f557dc1e6659c1d88613790bb3dddb5b/.
[v] K. Marten, "Russia's Use of Semi-State Security Forces: The Case of the Wagner Group," *Post-Soviet Affairs* 35, no. 3 (2019): 181, https://doi.org/10.1080/1060586X.2019.1591142.
[vi] C. Rondeaux, *Putin's Sledgehammer: The Wagner Group and Russia's Collapse into Mercenary Chaos* (PublicAffairs, 2025), 413.
[vii]J. Masters, "Ukraine: Conflict at the Crossroads of Europe and Russia," Council on Foreign Relations, February 14, 2023, https://www.cfr.org/backgrounders/ukraine-conflict-crossroads-europe-and-russia.
[viii] K. Stepanenko, *The Kremlin's Pyrrhic Victory in Bakhmut: A Retrospective on the Battle for Bakhmut* (Institute for the Study of War, 2023), https://understandingwar.org/wp-content/uploads/2025/04/A20Retrospective20on20Bakhmut20PDF.pdf.
[ix] The Times, "Wagner Group Mercenaries Admit Killing 40 Children in Bakhmut," April 18, 2023, https://www.thetimes.com/world/russia-ukraine-war/article/wagner-group-mercenaries-admit-killing-40-children-in-bakhmut-0903w6zx7.
[x] Office of the United Nations High Commissioner for Human Rights (OHCHR), *Treatment of Prisoners of War and Persons Hors de Combat in the Context of the Armed Attack by the Russian Federation against Ukraine: 24 February 2022 to 23 February 2023* (March 24, 2023), 9, https://www.ohchr.org/sites/default/files/documents/countries/ukraine/2023/23-03-24-Ukraine-thematic-report-POWs-ENG.pdf.
[xi] Meduza, "Human Rights Activist Releases Testimony from Two Wagner Group Mercenaries Who Describe Executing Ukrainian Civilians, Young and Old," April 17, 2023, https://meduza.io/en/news/2023/04/17/human-rights-activist-releases-testimony-from-two-wagner-group-mercenaries-who-describe-executing-ukrainian-civilians-young-and-old.
[xii] Institute for the Study of War, "Russian Offensive Campaign Assessment, April 24, 2023," April 24, 2023, https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment_24-16/.
[xiii] Rondeaux, *Putin's Sledgehammer*, 381–82.
[xiv] Rondeaux, *Putin's Sledgehammer*, 382.
[xv] J. Ber, *From Popasna to Bakhmut: The Wagner Group in the Russia–Ukraine War* (Centre for Eastern Studies, April 28, 2023), 1, https://www.osw.waw.pl/en/publikacje/osw-commentary/2023-04-28/popasna-to-bakhmut-wagner-group-russia-ukraine-war.
[xvi] L. Serwat, H. Nsaibia, and N. Gurcov, "Moving Out of the Shadows: Shifts in Wagner Group Operations around the World," ACLED, August 2, 2023, https://acleddata.com/report/moving-out-shadows-shifts-wagner-group-operations-around-world.
[xvii]Institute for the Study of War, "Russian Offensive Campaign Assessment, April 25, 2023," April 25, 2023, https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment_25-16/.
[xviii] M. Trevelyan, "Russia's Prigozhin Claims Capture of Bakhmut, Ukraine Says Fighting Goes On," *Reuters*, May 20, 2023, https://www.reuters.com/world/europe/russias-prigozhin-claims-full-control-bakhmut-2023-05-20/.
[xix] G. Faulconbridge, "Mercenary Prigozhin Says Kremlin Blanking Him on State Media Will Provoke Backlash," *Reuters*, May 28, 2023, https://www.reuters.com/world/europe/mercenary-prigozhin-says-kremlin-blanking-him-state-media-will-provoke-backlash-2023-05-28/.
[xx] Reuters, "Kremlin Denies Issuing Media with Guidance to Suppress Mentions of Mercenary Boss," February 16, 2023, https://www.reuters.com/world/europe/kremlin-denies-issuing-media-with-guidance-suppress-mentions-mercenary-boss-2023-02-16/.
[xxi] A. Mazurenko, "Reznikov on Surovikin's Dismissal: This Is Prigozhin's Conflict with Russia's Regular Army," *Ukrainska Pravda*, January 13, 2023, https://www.pravda.com.ua/eng/news/2023/01/13/7384713/.
[xxii] Institute for the Study of War, "Russian Offensive Campaign Assessment, April 25, 2023," https://understandingwar.org/research/russia-ukraine/russian-offensive-campaign-assessment_25-16/.
[xxiii] W. Letrone and T. Cabus, *The Wagner Group and the Question of the Legal Attribution of the Acts of Private Actors to a State* (HAL Open Science, 2025), 4, https://hal.science/hal-04885785v1/document.
[xxiv] C. Paul and M. Matthews, *The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It* (RAND Corporation, 2016), https://www.rand.org/pubs/perspectives/PE198.html.
[xxv] Rondeaux, *Putin's Sledgehammer*, 413.

[xxvi] F. Bryjka, "Tracing the Development of EU Capabilities to Counter Hybrid Threats," Polish Institute of International Affairs (PISM), 2022, https://pism.pl/publications/tracing-the-development-of-eu-capabilities-to-counter-hybrid-threats.

[xxvii] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (United Nations, 2001), art. 8, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

Photo: President Volodymyr Zelensky of Ukraine address the U.S. Congress. Kenny Holston/The New York Times

Lizi Tolordava

Ukraine's Information Operations: Winning over Narratives during the 2022 Russo-Ukrainian War

Information operations are the integrated use of computer networks, psychological influence and strategic communications. They can be used both in times of peace, as well as during active hostilities, from covert influence operations to instruments of hybrid warfare. Although the use of information operations in military confrontation is not a new phenomenon, in the hybrid conflicts of the modern era, information has transformed into a strategic weapon that can often have much faster and more effective geopolitical effects than conventional weapons have. The modern digital ecosystem has fundamentally changed the dynamics of war. Strategic narratives directly determine how global decision-makers perceive conflict, assess geopolitical risks and decide whether to provide vital military and financial support.

The full-scale invasion by the Russian Federation represents an unprecedented field of research into the use of information operations not just as a means of malicious use, but as a defensive mechanism. Both states are actively using the means of information warfare to gain dominance in the information sphere, although the Ukrainian experience has created a completely new precedent. It has shown how dominance over the information space can be turned into material-military support and why the institutionalization of strategic communications is a necessary condition for national defence and collective security planning.

The central thesis of the policy paper is that in the aforementioned war, Ukrainian information operations performed the primary defensive function of balancing and deterring the aggressor. Ukraine has managed to suppress the enemy's cognitive advantage, portray Russia as a global existential threat and gain a real military weapon.

The purpose of studying this issue is existentially critical for other vulnerable states just like Georgia, which has been a direct target of Russian hybrid aggression, occupation, borderization and continuous influence operations for decades. This policy document analyzes the mechanisms and political consequences of Ukraine's 2022 information operations in order to develop practical strategic recommendations for creating a shield for vulnerable states, while ensuring international security.

Historical and Strategic Background of Russian Hybrid Operations

The Russian Federation is a master of hybrid warfare, considering the information space as a constant combat domain, where the boundaries between peace and war are blurred. the Kremlin uses technical cyber operations and psychological influence before conventional warfare, during hostilities and even after the end of conflict. It was these information operations that based the dominant international narrative of the immediate military collapse of Ukraine at the early stages of the 2022 war. Such information dominance has created a critical security barrier, that prevented Western collective defense decision-makers from acting and disrupted the delivery of vital heavy military assistance.

The first large-scale practical use of this strategy in the post-Soviet era was carried out in Georgia during and after the 2008 Russo-Georgian war. Carrying out a complex hybrid arsenal against Georgia presents it as a direct target of Russian influence operations for decades and sets a clear example of how the aggressor prepares the ground for political and military aggression by destabilizing the information field.[i] Unfortunately, unlike Ukraine, Georgia didn't manage to implement information operations and strategic communication as a response measure and defense instrument.

Russia's information expansion in Ukraine is based on deep historical roots. Both in the Soviet and post-Soviet eras Russia systematically deployed the Russification of Ukraine and the discreditation of its cultural and national identity. For instance, the utilization of the Russified form of the names of the Ukrainian toponyms (such as

"Kiev", instead of "Kyiv") on the international stage resembled a tool to weaken Ukraine's sovereignty and to present Ukraine as a natural sphere of influence of the Kremlin.

The Pre-War Analytical Failure and the "72-Hour Fall of Kyiv" Narrative

While Russia has a long history of using various information operations, which was clearly demonstrated during and after the annexation of Crimea in 2014, these operations have assumed a particularly important role since the start of Russia's full-scale invasion on February 24, 2022. During this period, the narrative of Ukraine's imminent military collapse was dominant in the international society. This skepticism was largely due to the fact that Westerners relied almost exclusively on quantitative comparisons of military equipment and budgets in their assessments. This limited approach led to a false belief that "Kyiv would fall within 72 hours of a full-scale invasion". [ii]The position of global actors was consolidated around these pessimistic forecasts. According to assessments by the U.S. intelligence community, Russian forces could capture Kyiv in 96 hours, which would lead to the overthrow of the legitimate government and the establishment of a puppet regime, which would be loyal to the Kremlin.[iii] A similar position was shared by other leading international think tanks. As a result, the critics and the decision-makers overestimated the capabilities of the reformed Russian army and completely disregarded the operational progress, fighting spirit and social resilience achieved by the Ukrainian armed forces since 2014.

This prognosis had a direct negative impact on the political decisions of Western states. The uncertainty caused by the predicted collapse hindered the mobilization of international security assistance. For instance, at the time, the German government followed a strict restrictive stance against exporting weapons to crisis zones and was preventing Estonia from providing German-origin military support to Ukraine.[iv] The analysis of these processes provides a key political insight, since this skeptical forecast formed a critical security barrier. Thus, Russia's information advantage in the initial phase of the war disabled the mechanisms of international collective security. To combat this global skepticism, Ukraine immediately launched strategic information operations to prove its combat viability, change international approaches towards this war and ensure the mobilization of existentially necessary military contribution.

Overcoming the International Security Vacuum

The dominant global narratives revealed the fundamental weakness of the international security system. Traditional diplomatic approaches and slow mechanisms proved powerless to protect security against the Russian hybrid warfare. In this circumstances, Ukraine was forced to create an asymmetric defence mechanism that would counter the information adversary's dominance, shatter the portrayal of a weak state and influence the Western governments to change their positions through public pressure.

Ukraine's information operations became the main tool for balancing against the aggressor, self-preservation and mobilization of international support, which portrayed the aggression of the Russian Federation as a global existential threat, not only to Ukraine or a specific region and the war itself as a war to protect global peace and security. Its response was based on a coordinated and multifaceted strategic communication that influenced the political leadership, state institutions, the private creative sector, as well as civil society.

The first key factor was President Volodymyr Zelenskyy's direct digital diplomacy. Bypassing traditional diplomatic protocols, Zelenskyy formed a direct and authentic communication channel with a global audience through social media. A video address from Kyiv on February 26 in which Zelenskyy denied the disinformation about an evacuation and confirmed the presence of the high command on the ground, so he dispelled allies' doubts and invalidated Russian disinformation.[v] The President of Ukraine also addressed foreign parliaments and drew on the collective memory and security traumas of the targeted nations. While addressing the U.S. Congress and the Bundestag he used the allegory of Pearl Harbor and 9/11 and the Berlin Wall. [vi]

The second countermeasure was the use of nation branding as a defensive tool. The #KyivNotKiev campaign secured international recognition of Ukrainian toponymic sovereignty and within six months replaced Russified forms in the global media.[vii] The global campaign "Be Brave Like Ukraine",[viii] The "Made with Bravery"[ix] platform and the "Ukraine.ua" portal, created to ensure economic sustainability, transformed the intangible value of national bravery into a strategic resource.

The third means was to expose the adversary's moral degradation and logistical weakness. Ukraine became the first country to use official government accounts (@Ukraine, @DefenceU) for digital memetic warfare. By setting up the narrative of "David and Goliath" and presenting itself as the defender of democracy, while the

Russian army was presented as an immoral force. The visual documentation of the bombing of the Mariupol theater and the atrocities in Bucha coerced international institutions, such as ICC and OSCE, to launch war crimes investigations.[x] Also the exposure of 40-mile Russian military convoy's paralysis heading to Kyiv and the revelation of outdated Soviet maps finally shattered the myth of Russian military superiority.[xi]

The use of information operations as tools to manipulate the perceptions of international audiences has been used by the Kremlin for a long time. Particularly since the annexation of Crimea in 2014, most international relations and security researchers have focused exclusively on negative uses of information operations (disinformation, propaganda). However, information operations and strategic communications by militarily weaker states remains outside the sphere of academic attention. But the above-mentioned Ukrainian method of conducting information operations provides a unique precedent for how this instrument can effectively alter the narrative environment and international perceptions.

In fact, these operations managed to do something unpredictable: they exposed the fundamental violation of European security by the Russian invasion of Ukraine to a wide audience, while also exposing the systemic flaws of Western intelligence and analytical centers. This information victory led to a direct material transformation. The dominance gained by Ukraine in the global infosphere created unprecedented moral and political pressure in Western democratic societies, which forced them to fundamentally reconsider their defense policies. If in the initial phase of the war assistance was limited by the expectation that Ukraine would only put up guerrilla warfare, the new reality created by Ukrainians has allowed politicians to overcome their fears of escalation and begin delivering high-tech heavy weapons.

Recommendations

This Russo-Ukrainian War shattered traditional beliefs in the security sector and demonstrated that information power is the primary mechanism for national defense. Based on this experience, four key recommendations were made to strengthen the global security architecture and effectively counter hybrid threats:

- Since 2014, academic discourse has focused on Russian propaganda which has labeled information operations as a threat. The experience of Ukraine has shown

that a state can use information operations and strategic communications to expose the aggressor's brutality, attract coalitions and enhance public resilience. Actors such as academia, think tanks and NATO's Strategic Communications Center of Excellence should fill the existing theoretical gap and create a new research framework that examines positive and defensive functions of information operations.

- Each vulnerable state should develop a crisis information operations strategy, tailored not only to Russian aggression, but also to hybrid threats emanating from any authoritarian or revisionist state in general. National security councils and ministries of defense in countries facing existential and asymmetric threats should directly integrate strategic communications plans into defense systems. Strategic communication should become an integral part of the operational management of national defense in order to ensure proactive narrative dominance and mobilize allies from the very first minutes of a kinetic or hybrid escalation.
- The state should create formal partnership mechanisms with independent open-source intelligence researchers, civil activists and photojournalists. The Ukrainian experience has shown that visually verified documentation of war crimes and logistical failures attracts high trust in the global community.
- Security analysis must become more complex and realistic. The intelligence community and military analysts must quit superficial and unrealistic assessments of security issues that rely on dry theoretical knowledge, quantitative comparisons and material technical calculations. It must give equal weight to intangible factors, such as public resilience, fighting spirit and strategic communication skills. Western decision-makers must understand that when a real threat of aggression threatens a frontline or relatively small state, this is not just a local problem for that particular country, but threatens the entire global security. In reality, vulnerable states are critical links in a larger security chain. As the case of Ukraine shows, it is not just a single-country conflict, Ukraine is precisely the bridge and the barrier that holds back Russian aggression from moving forward.

CONCLUSION

This war confirmed that in a modern hybrid conflict control over the information field is a critical weapon that can both hinder and activate collective defense mechanisms. Ukraine's strategic information operations such as: portraying the Kremlin as a global existential threat and neutralizing Russia's information dominance, fundamentally reshaped the system of perception of international security. For countries, such as Georgia, this experience is not an abstract theory, but a practical survival guide against the constant Russian information operations. Therefore, defense must also be constant and proactive by creating an institutionalized information shield.

Photo: Zelensky records a video message at the entrance to Kupiansk, Kharkiv region, December 12, 2025. Ukrainian Presidential Press Service

[i] Shakarian, Paulo. (2011). *The 2008 Russian Cyber-Campaign Against Georgia.* https://www.researchgate.net/publication/230898147_The_2008_Russian_Cyber-Campaign_Against_Georgia

[ii] Heinrich, J., & Sabes, A. (2022, February 5). Gen. Milley says Kyiv could fall within 72 hours if Russia decides to invade Ukraine: Sources. *Fox News.* https://www.foxnews.com/us/gen-milley-says-kyiv-could-fall-within-72-hours-if-russia-decides-to-invade-ukraine-sources

[iii] Brennan, D., O'Connor, T., & Jamali, N. (2022, February 24). Exclusive: U.S. expects Kyiv to fall in days as Ukraine source warns of encirclement. *Newsweek*. https://www.newsweek.com/us-expects-kyiv-fall-days-ukraine-source-warns-encirclement-1682326

[iv] Gordon, M., R., & Pancevski, B. (2022, January 21). Germany blocks NATO ally from transferring weapons to Ukraine. *The Wall Street Journal*. https://www.wsj.com/world/europe/germany-blocks-nato-ally-from-transferring-weapons-to-ukraine-11642790772

[v] ZelenskyyUa [@ZelenskyyUa]. (2022, February 26). https://x.com/ZelenskyyUa/status/1497450853380280320

[vi] Dyczok, M., & Chung, Y. (2022). Zelens′kyi uses his communication skills as a weapon of war. *Canadian Slavonic Papers*, *64*(2–3), 146–161. https://doi.org/10.1080/00085006.2022.2106699

[vii] Barnett, L. (2024). *#KyivnotKiev: An investigation into British politicians' pronunciation of Ukraine's capital city and the influence of political ideology on variation* (Long dissertation, English Language). Newcastle University, Excellent Language and Linguistics Dissertation Repository. https://blogs.ncl.ac.uk/elldr/files/2024/09/Barnett2024.pdf

[viii] Carat. (n.d.). *Be brave like Ukraine: A global solidarity campaign*. Carat. https://www.carat.com/work/be-brave-like-ukraine

[ix] Ministry of Foreign Affairs of Ukraine. (2022, September 13). *Made with bravery. Бізнес за підтримки Мінцифри та МЗС запустив маркетплейс для просування українського експорту*. https://mfa.gov.ua/en/news/made-bravery-biznes-za-pidtrimki-mincifri-ta-mzs-zapustiv-marketplejs-dlya-prosuvannya-ukrayinskogo-eksportu

[x] Scholz, J.-P. (2026, March 30). Ukrainian photographer who risked all to film Bucha massacre. *Deutsche Welle*. https://www.dw.com/en/ukraine-bucha-massacre-kyiv-russia-war-crimes-photographer-full-story/video-76598852

[xi] Press, C., & Libet, S. (2023, February 22). *How Russia's 35-mile armoured convoy ended in failure.* BBC. https://www.bbc.com/news/world-europe-64664944

Photo: U.S. Army Special Operation Forces during the exercise Saber Junction 2019 in Germany. U.S. Army photo by Spc. Patrik Orcutt

Davit Bakradze

The Impact of Influence Operations and Hybrid Means on Conventional Warfare

Modern wars, unlike those that took place before the 21st century, have radically changed in nature. War is no longer merely a confrontation between the military forces of two countries on the battlefield; today, it is much more complex and difficult to understand. Factors that increase this complexity include covert and overt informational and psychological operations, as well as the growing significance of cyberattacks, influence operations and hybrid methods. Wars have shifted into a new dimension in which fighting and defense have become even more challenging, especially for relatively small states.

The relevance of this topic is underscored by Russia's 2022 invasion of Ukraine and the outbreak of the largest conventional war since World War II. The invasion involved numerous tools of influence operations and, subsequently, various hybrid warfare methods that are still actively used against Ukraine today. This war serves as one of the clearest examples for analyzing military and political issues. I will follow this approach and, by examining the largest war of the 21st century, attempt to demonstrate my thesis: hybrid methods have influenced the transformation of conventional warfare and created additional challenges for states engaged in war.

This paper will explain the mechanisms and objectives of Russian influence operations, describe the various operations planned and executed by Russia against Ukraine and clarify the role that the Russian Federation assigns to influence operations. Additionally, I will seek to show how a target country can counter such threats and answer the following research question: How have hybrid methods changed conventional warfare, using Ukraine as a case study?

Russian Influence Operations and 24 February

Before turning to the main discussion, it is necessary to briefly outline the definitions of and distinctions between influence operations and hybrid warfare. Hybrid warfare is a type of conflict in which conventional military operations are combined with a full spectrum of unconventional tools, ranging from terrorist activities to cyberattacks.[i]

Influence operations, by contrast, refer to coordinated diplomatic, informational, economic and other non-military actions undertaken during peacetime and directed at a target state with the aim of shaping attitudes and behaviors among its population.[ii]

Russia has extensive experience and a long history of employing hybrid instruments. As early as the 1950s, the term "active measures" emerged, referring to the use of subversive tactics against the governments of target states, support for favorable political movements and, most importantly, the systematic dissemination of disinformation.[iii]

After the collapse of the Soviet Union, its legal successor, Russia, continued and further developed the techniques initiated by the communist regime. Russia is believed to have been involved in orchestrating a military coup in Georgia and subsequently to have used proxy forces to occupy Abkhazia. Later Russian activities included attempts to interfere in elections in Ukraine, the 2008 war, the 2014 annexation of Crimea and the destabilization of Donbas and Luhansk.[iv]

Following the occupation of these territories, a period of positional confrontation began, accompanied by an unprecedented escalation of influence operations against Ukraine. This marked the beginning of preparations for the events leading up to 24 February.

Among Russia's influence tools, information and psychological warfare require special attention. Information campaigns targeted both the Ukrainian and Russian

populations. On the one hand, the objective in Ukraine was to generate anti-government sentiment, convince the public of the authorities' incompetence and corruption and undermine trust in state institutions. In addition, efforts were made to evoke nostalgic sentiments, particularly among the elderly, regarding historical ties between Russians and Ukrainians and notions of shared identity. These efforts also included the instrumentalization of religious sentiments, actively supported by the Russian Orthodox Church. Prior to the invasion, numerous churches and clergy subordinate to Moscow were operating in Ukraine.[v]

In Russia, the aim was to cultivate the opposite perception. A massive flow of narratives portrayed Ukrainians as "fascists" who allegedly oppressed Russian-speaking communities, murdered civilians and tortured prisoners.[vi]

Yet psychological warfare was arguably the most important component. Psychological pressure was intended to play a decisive role at the outset of the conventional invasion and in its subsequent phases. Russia presented itself, both domestically and to international observers, as an unstoppable military machine. Many Western experts echoed this perception. In the West, it was widely believed that the Ukrainian Armed Forces would be unable to offer substantial resistance and that Kyiv would fall within three days (NATO Secretary General Jens Stoltenberg). These narratives were reinforced by the large-scale mobilization of Russian forces near the border and continuous military exercises, which increased psychological pressure on the Ukrainian population.[vii]

It is important to analyze how influence operations and hybrid tools shaped the conventional phase of the war and its initial trajectory. Russia's military strategy was premised on the assumption that hybrid operations had already broken Ukrainian defenses. Information and psychological terror aimed to convince Ukrainians that their armed forces would not withstand Russian attacks and that the capital would fall within three days. Russian media, troll factories and social networks were widely employed, supplemented by statements from Western military analysts. This fueled Russia's belief that a blitzkrieg was possible. Airborne, mechanized and armored units advanced directly toward Kyiv, bypassing potential direct engagements in an attempt to reach the city rapidly. As later became clear, Western assessments were incorrect, and Russia's own information and psychological campaign failed, contributing to the collapse of its military operation.[viii]

Can these developments be viewed as a victory for the Ukrainian people, or were they merely a coincidence? There is no definitive answer. However, a careful analysis of the situation may help identify how the Russian military machine can be halted before it gains momentum.

Broken Russian Plans and Ukraine's Hybrid War

Russia's main expectation did not materialize. Ukrainian soldiers chose to fight, and the government remained in Kyiv. Most importantly, the people decided to fight because no one else could defend their country. Millions left the country, but most of them were women and children.

The blitzkrieg, through which Russia expected to reach Kyiv without resistance and win easily after minor clashes, collapsed. Why did the Russian strategy fail, and why did its plan to win the war fall apart? At first glance, the answer is simple: hybrid tools were not used effectively enough to transform conventional war and turn it into a march toward Kyiv. Had its influence operations succeeded, Russia's plan would have been straightforward: an information and psychological campaign would have crushed Ukraine's will, and the demoralized country would have surrendered to the advancing Russian army. To explain why this did not happen, we must examine the experience and psychology of the Ukrainian nation.

Since 2013, Ukraine has been in open or covert confrontation with Russia. Kyiv endured the Maidan, lost Crimea and had to fight in Luhansk and Donetsk. For nine years, the country went through many difficult periods. A national identity formed among Ukrainians—one shaped by centuries-long resentment toward Russia. This experience is likely one of the main reasons why the army and the people remained and why Russian information warfare could not break them.

Another important factor is the Ukrainian people's moral readiness to resist the invading enemy. The population did not rely solely on state structures. Ordinary people tried to act independently and contributed to the defense. This may explain why Russian "deepfake" attempts suggesting that Zelensky had fled the country failed.[ix]

Another contributing factor is practical experience: years of disinformation campaigns targeting Ukrainians effectively trained them. Russian security services could no longer easily convince them of narratives that did not correspond with reality. At the same time, the Azov Regiment and other military units had years of experience fighting

Russian forces, especially on the eastern front, so the situation did not change dramatically for them.

Additionally, the work of the President, the Presidential Administration and city mayors must be highlighted. Officials maintained constant communication with the population through briefings, official statements and live broadcasts on social media. They demonstrated that they remained in Ukraine and continued to fight, which strengthened the already high levels of motivation and trust among the population.

Ukraine itself used influence-operation tools relatively successfully. First, through information campaigns, it built positive attitudes in the West, which helped attract military support from European leaders. The second major achievement was on the battlefield. Starting in spring 2022, Ukraine planned a counteroffensive that targeted the southern front to liberate Kherson and Zaporizhzhia. Officials talked about this plan and it was heavily circulated by troll-bot networks on social media. In wartime, such statements are usually inexpensive, but Ukraine supplemented them with real actions. Several brigades armed with Western equipment were moved to the southern front, creating the impression that Kyiv was preparing to launch a counteroffensive. This strategy worked: the Russian command redeployed forces southward and Ukraine quickly responded with an offensive in the north, liberating Kharkiv in a short time.[x] Similar attempts followed, but the Zaporizhzhia campaign ultimately failed.[xi]

What Could Have Been Done Better and What We Should Do

Ukraine endured Russia's hybrid assaults largely by relying on accumulated experience, supported by several sound decisions made by its political leadership and the strong emotional resilience that Ukrainians demonstrated during the early days of the war. However, an important question remains: what should be done during times of peace? And how can Georgia prepare to counter similar threats?

A significant body of scholarship argues that, in hybrid warfare, offensive action is generally more effective than remaining in a defensive posture. When a state remains on the defensive, Russia retains the initiative to determine when, where and how to strike.[xii]

It is essential that greater resources be allocated to monitoring and detecting such threats. Early identification of the source of a problem gives the targeted state more time to neutralize it and substantially increases its chances of success. This is especially

relevant in the field of information warfare and in identifying infiltrated agents. For example, after the outbreak of the war in Ukraine, the government initiated efforts to expose covert Russian agents embedded within the Russian Orthodox Church who were actively involved in spreading propaganda and disinformation. These operations frequently triggered sharp reactions from Russia, further highlighting the church's instrumental political role. Some arrested clergy were even found to have participated in guiding missile strikes.[xiii]

Responding to attacks with counterattacks also proved effective in Ukraine. In the early stages of the war, Ukraine actively disseminated videos of wounded or killed Russian soldiers, along with footage of Russian prisoners of war describing the humane treatment they received from Ukrainian forces. While such methods alone are unlikely to cause the collapse of the Russian military, there were dozens of confirmed cases of Russian soldiers surrendering. Ukraine even created a reward system for the surrender of Russian military equipment, leading to verified instances of Russian servicemen handing over several pieces of heavy weaponry, including a helicopter.

What should Georgia do? In Georgia, Russian psychological operations have been notably successful. Despite the fact that the country does not face an immediate threat of war, even the mention of it causes public panic, and many prefer to avoid discussing the topic entirely. In the event of a real military confrontation, such attitudes could lead to societal breakdown and military defeat. Therefore, the primary priority must be to address these psychological vulnerabilities and actively shape public attitudes. War is indeed a tragic and devastating phenomenon, but even more catastrophic would be the rampage of the Russian military against civilians, the loss of independence and freedom and, as seen in Chechnya and other regions, the forced conscription of citizens into a foreign army. The only way to prevent this is through the dissemination of accurate, well-structured information tailored to Georgian society through the media. It is essential to raise morale and remind citizens that, despite enduring numerous wars throughout history, Georgia continues to exist.

The second essential component is countering information warfare. Georgian society remains highly vulnerable to Russian disinformation and can easily become a target of manipulation. Comprehensive information campaigns, as well as training programs for both public- and private-sector institutions, are necessary.

The Russia-Ukraine war demonstrated that modern warfare begins long before it becomes visible. If a state fails to engage in the conflict during its early stages, it faces the risk of losing before the war officially begins.

CONCLUSION

Influence operations and hybrid warfare tools had a profound impact on the Russia-Ukraine military confrontation. Russia based its military campaign almost entirely on the success of hybrid tactics, while Ukraine's information warfare efforts played an important role in enabling its counteroffensive operations. Future wars will rely even more heavily on such hybrid methods, and states must devote greater attention to defending themselves against these threats.

It is crucial that Georgia internalize these lessons as well. The country's defense capabilities have been declining year by year, while society has become increasingly vulnerable to hybrid threats. The recommendations outlined in this paper represent only a framework that must be continually developed and refined by the nation's security institutions. The education system also has an important role to play in this context, although, given current circumstances, meaningful progress appears unlikely in the near future.

Photo: A Ukrainian soldier prepares a reconnaissance drone at a combat position in Donetsk Oblast, Ukraine, January 22, 2026. Diego Herrera Carcedo/Anadolu via Getty Images

[i] Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (Arlington, VA: Potomac Institute for Policy Studies, 2007), 8, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[ii] Eric V. Larson et al., *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (Santa Monica, CA: RAND Corporation, 2009), 12, https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

[iii] Galeotti, M. (2019). *Active measures: Russia's covert geopolitical operations.* George C. Marshall European Center for Security Studies. https://www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0

[iv] Cordesman, A. H., & Hwang, G. (2020). *Chronology of possible Russian gray area and hybrid warfare operations* (CSIS Report No. RR 24779). Center for Strategic and International Studies. https://www.jstor.org/stable/resrep24779

[v] Малюк, В. (2022, October 27). Керівник СБУ Малюк: Просто ми, українці, дуже любимо бавовну. *Інтерфакс-Україна.* https://interfax.com.ua/news/interview/868357.html

[vi] Snegovaya, M. (2015). Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare. *Institute for the Study of War.* https://www.jstor.org/stable/resrep07921.1

[vii] BBC News. (2022, February 11). Ukraine tensions: Russia stages military drills with Belarus. *BBC.* https://www.bbc.com/news/world-europe-60327930

[viii] Ionita, C. C. (2023). Conventional and hybrid actions in the Russia's invasion of Ukraine. *Security and Defence Quarterly, 44*(4), 5-20. https://doi.org/10.35467/sdq/168870

[ix] Kofman, Mike. (2025, January 25) How Russia's Military Is Being Worn Down by the War. Decoding Geopolitics Podcast with Dominik Presl. https://www.youtube.com/watch?v=Vj6oiILlJrY

[x] President of Ukraine. (2022, September 14). *President took part in the ceremony of raising the State Flag in de-occupied Izyum.* Official website of the President of Ukraine. https://www.president.gov.ua/en/news/prezident-uzyav-uchast-u-ceremoniyi-pidnyattya-derzhavnogo-p-77769

[xi] Zaluzhnyi, V. (2025, September 24). *Роль інновацій як основи стратегії стійкого опору у позбавленні Росії можливості нав'язувати свої умови через війну.* ZN.UA. https://shorturl.at/jymCb

[xii] Stijnman, E. (2025, July). *Countering Russian hybrid warfare: The best defence is a good offence.* Clingendael Institute. https://www.clingendael.org/sites/default/files/2025-07/Countering_Russian_hybrid_warfare.pdf

[xiii] Kirby, P. (2022, November 8). Why did Putin's Russia invade Ukraine and how could the war end? *BBC News.* https://www.bbc.com/news/world-europe-63715922

Photo: Israeli ground troops during the Second Lebanon War, August 2, 2006. Pierre Terdjman/Flash90

Rati Mamaladze

Hybrid Warfare and the Changing Nature of Conflict: Implications for State Security on the Case of Hezbollah-Israel Conflict of 2006

Hybrid warfare is the blending of conventional military force with unconventional non-kinetic tools by a non-state or a state actor. This synchronized multimodal approach creates severe and complex challenges that traditional defense structures are not built to counter. In the postmodern world, where hybrid warfare has become a defining feature of many conflicts, the 2006 Israel-Lebanon war was one of the clearest early prototypes: a non-state actor caught the superior military off guard and managed to push it to the limits. Its relevance reached beyond Israel and pushed security planners worldwide to reassess their doctrines in order to prepare themselves for the emerging challenges of hybrid warfare.

Against this background, the policy paper addresses the research question: to what extent did Hezbollah's hybrid warfare strategy in the 2006 conflict expose vulnerabilities in Israel's and global state security frameworks? By analyzing the military, legal and informational dimensions of the conflict, the paper will demonstrate the capabilities of hybrid actors to neutralize conventional advantages through non-conventional means, such as the exploitation of doctrinal rigidities, shaping perception and weaponizing international law.

From Resistance to Hybrid Warfare: Hezbollah's Transformation

For over 20 years Israel waged a military campaign against Lebanon. In 1982 Israel Defense Forces (IDF) under the operation PEACE FOR GALILEE invaded Lebanon with the sole intent of eliminating the threat emanating from the Palestine Liberation Organization (PLO) by incapacitating it completely, starving it from the ability to wage any type of war. Israeli heavy divisions moved into the Northern outskirts of Beirut killing numerous PLO members and sending the rest into retreat, as the Israeli Air Force (IAF) actively in tandem targeted Syrian air defense systems on Lebanese soil. The PLO never recovered after 1982. Initially, the IDF was met with open arms by the Lebanese population, pictured as liberators, however, the attitude did not last long as the Israeli occupation soon turned bitter, and respectively to this issue the reaction was the creation of a Shiite faction Hezbollah, a militia force trained, armed and equipped by Iran and Syria[i].

Hezbollah was determined to drive IDF out of Lebanon and after numerous clashes and loss of life on both sides in June 2000 United Nations Interim Force in Lebanon (UNIFIL) established a new border line between the respective states - a 79-kilometer demarcation or a withdrawal boundary, which was endorsed by the UN Security Council. Israel abided and withdrew its forces in accordance with the Security Council resolution 425. Nevertheless, suspicions remained high within the Lebanese government towards Israeli intentions, and due to this the war-making capabilities of Hezbollah was maintained in southern Lebanon with direct support from Syria and Iran[ii].

Following the withdrawal, Hezbollah internalized, that diplomatic efforts, U.S. promises and UN involvement did not liberate Lebanon, but resistance and public support did – with that knowledge and no active guaranteed deterrent, the militia directed all of its resources towards preparing for the next confrontation with Israel. Hezbollah spent the following six years constructing a hybrid military machine, which was a deliberate doctrine-driven transformation. Iran and Syria supplied between 12,000 to 13,000 short, medium and long-range missiles – which Hezbollah would operate with newly acquired dispersal and firing systems specifically designed to survive Israeli airstrikes. Over 600 bunkers and tunnel networks were constructed with the assistance of the Iranian Revolutionary Guard and North Korean supervisors, with complex compartmentalization designed to withstand precision airstrikes.

Additionally, Hezbollah was supplied with anti-tank missiles including the Kornet-E, integrated with mines, improvised explosive devices (IEDs) and indirect fire, which was specifically designed for halting Israeli armored advancements. Hezbollah's Secretary-General Nasrallah expressed that this was not a regular army, nor did it operate as a guerilla force, rather it was something in the middle, representing a new model[iii].

The said new model was characterized by Frank Hoffman through the definition of Hybrid Warfare, a concept which he described as simultaneous and adaptive use of tailored mix of conventional weapons, irregular tactics, terrorism and criminal behavior, by a state or a non-state actor, within the battlespace with the aim of achieving specific political objectives. A multi-modal approach that blurs the line between peace and war, combining the utility of conventional military force with non-conventional methods[iv]. Hoffman, essentially, defined hybrid warfare on the 2006 Hezbollah-Israel war example, using the modus operandi of the Shiite faction as its prototype. The 2006 conflict was the clearest depiction of the changing nature of conflict with Hezbollah as a modern hybrid challenger of a militarily superior state. During the 34 days of war, Hezbollah proved to be "maddeningly elusive" to Israeli troops. It fired over 4,000 rockets into Israel territory across the span of the conflict; 18 Merkava Mark IV tanks were damaged by anti-tank missiles, which at the time was Israel's most advanced armor; the IDF launched over 19,000 sorties and dropped over 20,000 bombs, yet failed to neutralize Hezbollah. Hoffman explicitly emphasizes the importance of the battle for perception alongside the military contest, he covers Hezbollah's unique approach towards media coverage in real time, like the magnifications of limited tactical success and minimization of heavy losses, essentially creating a lopsided information environment, where Israel lost complete control over the narrative despite winning the battles. The Winograd Commission, with the culmination of the conflict, made a post-mortem report on decision-making processes and civil-military interactions throughout the contest. Significant flaws were uncovered in the process, information content, information flow and resulting decisions at the strategic level – which brings us to the core problem, a small-scale organization managed to face down one of the strongest conventional armies in the world through innovative approaches, which spurred the contingent of security planners around the world towards change and adaptation[v].

The Hezbollah Model: Multidimensional Challenges to State Security

The Military Dimension

Central weaknesses that was exposed during the 2006 conflict was Israel's reliance on a flawed operational doctrine. Effects-Based Operations (EBO) and Systemic Operational Design (SOD) were two strategic concepts that were strictly embraced by the IDF prior to the war, which emphasized prioritized usage of airpower and technological superiority over conventional ground troop utilization. Dependence on airpower would prove ineffective in conflict against a decentralized and a flexible adversary, the assumption stems from the fact that airpower alone would not disperse or eliminate Hezbollah. Extensive aerial bombardment did not incapacitate the militia, which managed to maintain its ability to launch rockets in Israeli territory. From a broader perspective, this reveals a critical deficiency in state security frameworks that technological superiority alone is not effective against hybrid threats. Second major issue derives from IDF's gradual erosion of conventional combat readiness. After years of counterinsurgency operations in Palestinian territories, the Israeli ground forces "lost" their ability to fight a "real war". IDF shifted its doctrinal focus on policing and readiness towards low-intensity clashes, and when faced with a quasi-conventional opponent with high level organization, the conventionally superior army failed to mitigate its pressure. Thus, exposing that modern militaries tend to experience reduced adaptability with prolonged exposure to one type of conflict, which Hezbollah exploited through hybrid warfare. Israel's rigidity in conflict was easily seized by Hezbollah with its unique operational characteristics, like the usage dispersed rocket-launching systems. Personnel could deploy, set up, fire and relocate in a matter of half a minute. In such a short timeframe Israeli air power could barely locate the target deeming its airstrikes ineffective. Furthermore, the integrated system of anti-tank mines and guided missiles (ATMGs), Kornet-E, immobilized the core advantage of IDF, which was its armored division, halting majority of its ground advancements, thus highlighting the redefinition of asymmetry, it is not about mere weakness rather intelligent adaptation to an environment, simply put – weakness is deliberately translated to efficacy through intelligent choices. Another critical issue rises from Israel's strategic miscalculation and intelligence discrepancies. Hezbollah's capabilities and intentions were misread by Israel security planners, all of whom presumed that this would be a quick and decisive campaign. With little to no knowledge about Hezbollah's military buildup and its intentions of sustaining a long confrontation,

Israel engaged in conflict with insufficient preparation. Such misjudgments cultivate advantageous environments for hybrid actors to thrive in, the exact gap in perceptions and actual capabilities, creates a structural problem for state security. And lastly, the ambiguity of the doctrines. The SOD caused significant problems within the IDF and command structures due to its abstract integrity and unusual philosophical derivatives. Poorly understood conceptual documents essentially made it difficult for IDF officers to grasp its design and contents (an institutional shortcoming), which created a broader practical issue, the complex doctrine could hardly be translated into effective battlefield performance[vi].

The Legal/Ethical Dimension

Crucial part of 2006 Israel-Hezbollah conflict was the conjunction of hybrid warfare and the international humanitarian law. The international Committee of Red Cross has coined a term called "human shields" which describes a method of warfare when a subject deliberately utilizes highly urbanized areas with present civilian population and movement in order to shield its critical military objectives and infrastructure from an attack, a practice which is clearly prohibited under the rules of armed conflict[vii]. During the conflict, with clear empirical evidence, Hezbollah used the Lebanese civilian population as "human shields" by emplacing weapons, fighters, infrastructure and equipment in civilian areas with the intent of deterring an attack from the IDF, clearly a violation of humanitarian law. The documented cases varied from storing, shooting and firing weapons from inside heavily populated areas, which disregarded even the modicum of precautions needed to be taken by a subject to prevent loss of civilian life[viii]. While questions remain about the extent to which this constituted as an intentional breach of international humanitarian law, such practice caused significant issues in differentiating combatants and civilians, complicating Israeli targeting decisions.

International humanitarian law obliges military forces to distinguish civilian and hostile targets and to ensure proportionality in the use of force, which created a significant structural dilemma for IDF. Hezbollah's intentional entrenchment in civilian areas guaranteed that any attack conducted by the IDF would result in collateral damage (civilian causalities), thus each attack carried not only tactical consequences but moral and reputational costs. Within that analytical framework, rules of armed conflict turned into a battlespace itself, which was exploited by Hezbollah, essentially, constraining its

adversary by leveraging civilian proximity and increasing political and moral costs of every intended attack, overall impeding military advances. This created a consequential precedent, rules of war were manipulated by a hybrid actor in a way that created advantages, and moving forward can be used against democracies, that inherently are law abiding.

The Information Dimension

Another crucial element in the Lebanese conflict was the usage of media, showing its potential as a legitimate and an effective weapon in a guerilla conflict. "We see the media battle as equally important to the fighting on the ground" told Manar chief Nayef Krayem in October 2000. The TV channel Al Manar identifies itself as a "station of resistance" used to wage "psychological warfare against the Zionist enemy". The channel actively shaped the narrative of war[ix]. The same messages were reinforced by the Secretary-General Hassan Nasrallah in his carefully calibrated speeches, in which he further accentuated the Hezbollah cause, he influentially used rhetoric of resistance against oppression to justify the measures taken, framed events as "victories" which were sometimes difficult to dispute and extensively focused on the greatness of resisting martyrs, all of which helped garner regional and domestic support[x].

Hezbollah's information strategy was not a mere improvisation but rather part of a broad strategy deeply integrated into its operational approach. The organization treated media coverage and communication as central part of warfare as explicated in the preceding paragraph, which were aimed at influencing public perceptions and opinions. Systematic projections of resilience and deliberate positive reinforcements of certain events helped Hezbollah create an information environment where it was the one pulling the strings, thus being able to construct a narrative of victory and success. Despite experiencing significant material losses, Hezbollah managed to win the war of information and undermine Israel's image of superiority.

This example underlines that the information domain can be an active battlespace. If one side struggles to successfully "advertise" its military successes through strategic communication, the one who dominates the perception can have consequential effects on the outcome of the war. This dynamic highlights that control over territory is of similar importance as control of the information environment, one can win the battle through military superiority, but the other can win the war through information, as it can have profound effects on international legitimacy and pressure, and domestic

morale and support. Thus, the information space is a warfighting domain, not an afterthought or an addition.

Recommendations

1. Developing Hybrid-Defense Force Structures

Conventional armies require dedicated units or divisions within their rank and file specifically meant for countering hybrid opponents. Their mode of operation will not purely focus on counterinsurgency or conventional warfare, but rather their amalgamation.

Implementation of such policy requires a state to hold systemic training exercises under joint structure of armored units, urban warfare specialists, intelligence and informations officers. The main operative groups will learn how to effectively engage in close quarter combat (CQC), how to clear out and map intricate tunnel networks and fully utilize ground maneuvers when the enemy objectives are shielded by civic infrastructure and civilians, especially in circumstances when air superiority proves ineffective.

Implementation of such policy will allegedly face risks and obstacles which vary from budget constraints to institutional resistance to doctrinal change, however, the biggest risk would be the over-preparation for the last war rather than the next one. Hybrid warfare does not entail similar mode of operation in every conflict, it suggests adaptability, flexibility and uniquity that comes with every confrontation, meaning that whatever might have worked against Hezbollah in 2006 might not work elsewhere or in another conflict with a different actor also engaging in hybrid warfare. Thus, doctrinal manipulation must not be rigid, but rather flexible and open to circumstantial adaptation.

2. Closing Intelligence and Analytical Gaps

States require better frameworks for assessing and closing the gap between the perceptions of and realizable capabilities. Easily accessible information about adversary's arsenal, its ability to use them and how and when they will use them creates a useful benchmark for security planners to build upon. Implying that when the state is aware, it can meet the challenger prepared without overburdening its engagement with myriads of technical and non-technical assets, thus tailoring each response according to the available intelligence.

Policy implementation will take place within intelligence services with the addition of dedicated hybrid threat assessment units or groups. Team exercises will specifically help influence habitual, or to a certain extent heuristic, behavioral changes in regard to assumptions about non-state actors. To clarify, intelligence officers will be less inclined to abide by certain biases and will carefully assess the situation.

Unfortunately, intelligence reform will not fundamentally resolve the issue. Intelligence discrepancies can be traced back to human cognitive errors, like in the IDF case, intelligence officers were aware of Hezbollah's possession of Kornets, yet they did not believe that a non-state actor could effectively operate them.

3. Institutionalize Information Operations

Strategic communication should not be considered as an afterthought, counter-narrative capabilities should be built into the defense planning from the start due to its importance, since it can have consequential effects on the outcome of the war, setting a baseline that the information space carries similar strategic weight as for example a strategically important territory.

Reactive response to information war will not bring positive results, thus the following reforms should be implemented – creation of information operation units, dedicated pre-planned media strategies for specific conflict scenarios and rapid response communication.

However, such policy can create tensions for democracies that should be explicitly pointed out. State-controlled outlets and state-linked channels that engage in narrative control might risk conflict with press freedom, which can eventually erode public trust. In essence such policy implementation should undergo significant scrutiny and deliberation until it is ready to be implemented.

CONCLUSION

The 2006 conflict was a turning point that demonstrated hybrid warfare is not theoretical but a replicable reality that exposed deficiencies in state security planning. Hezbollah utilized three dimensions of conflict and demonstrated, in military terms, that technological superiority and flawed doctrine are insufficient for mitigating pressures from a hybrid challenger. The ethical/legal dimension demonstrated that the rules of war can be used as a weapon by a hybrid actor, which can be exploited for advantage. Lastly, the information dimension proved that the information space can exert influence beyond its domain, and narrative control carries equal strategic weight to battlefield performance.

To address these vulnerabilities, three recommendations can be applied: first, restructure and align forces to hybrid threats; second, close analytical and intelligence gaps in institutions and independent agencies; and third, treat the information domain as a core defense area rather than an "inhibitor."

This can be achieved through dedicated training exercises and facilities, doctrinal reform, intelligence restructuring and pre-planned strategic communications frameworks with robust network systems.

The lessons of 2006 are not historical but rather ongoing. Hezbollah's model has been studied and emulated by many non-state actors and states themselves. It has been observed globally. The question now no longer revolves around whether hybrid warfare will be encountered – it already has. The relevant question in current circumstances is whether states have adapted proactively or reactively. The 2006 conflict was the clearest warning; the cost of ignoring it compounds over time.

Photo: Reuters: Gil Cohen Magen

[i] Matthews, M. M. (2008). We Were Caught Unprepared: The 2006 Hezbollah-Israeli War. Washington DC: Combat Studies Institute (CSI). (pp. 6-7)
[ii] Matthews, M. M. (2008). We Were Caught Unprepared: The 2006 Hezbollah-Israeli War. Washington DC: Combat Studies Institute (CSI). (pp. 7-16)
[iii] Matthews, M. M. (2008). We Were Caught Unprepared: The 2006 Hezbollah-Israeli War. Washington DC: Combat Studies Institute (CSI). (pp. 16-22)
[iv] Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, Virginia: Potomac Institute for Policy Studies. (pp. 4)
[v] Hoffman, F. G. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, Virginia: Potomac Institute for Policy Studies. (pp. 35-42)
[vi] Matthews, M. M. (2008). We Were Caught Unprepared: The 2006 Hezbollah-Israeli War. Washington DC: Combat Studies Institute (CSI).
[vii] ICRC. (2025). Human Shields. Retrieved from How does Law Protect in War?: https://casebook.icrc.org/a_to_z/glossary/human-shields
[viii] ICRC. (2006, November 23). Israel/Lebanon/Hezbollah Conflict in 2006. Retrieved from How does Law Protect in War?: https://casebook.icrc.org/case-study/israellebanonhezbollah-conflict-2006
[ix] Fontana, L. (2010, March 30). Conflicting Information Strategies in the 2006 Lebanese War. Retrieved from Arab Media & Society: https://arabmediasociety.com/conflicting-information-strategies-in-the-2006-lebanese-war
[x] Abu-Lughod, R. A., & Warkentin, S. (2012). Understanding Political Influence in Modern-Era Conflict: A Qualitative Historical Analysis of Hassan Nasrallah's Speeches. Journal of Terrorism Research, 32- 47.

Photo: BBC/Getty Images

Lizi Oniani

Russia's Influence Operations Against Georgia: Understanding Hybrid Threats and Strategic Thinking

Russia has always viewed Western, democratic states as a threat that could limit its imperialist views and borders as a state. This became a particular problem for Russia when its neighboring post-Soviet countries decided to adopt a Western course. One such state is Georgia. Currently, the biggest challenge to Georgia's security is the Russian Federation, which considers Georgia to be its sphere of influence. The development of technologies in the 21st century and the active conduct of hybrid warfare have somewhat simplified for Russia the use of unconventional warfare methods to weaken Georgia's statehood and democracy. Russia's main interest is to stop the enlargement of the EU and NATO, which includes Georgia and its aspirations to follow a Western course and unite under the Western wing. For Russia, it is a strategic task to keep Georgia in its sphere of influence.

The research question of the article is the following: How do hybrid threats against Georgia help Russia to maintain its influence in the wider Black Sea region?

Georgia's place in Russia's Strategic Thinking

Russian imperialism, deeply rooted in Russian society and governments, did not disappear even after the collapse of the Soviet Union. After its collapse, Russia considers the post-Soviet space as its sphere of influence and tries not to lose relevance in these countries and regions. This is the reason why Russia waged war in Georgia in 2008, after the Bucharest Summit increased the chances of Georgia joining NATO. The same happened in Ukraine in 2014, when Russia annexed Crimea and in 2022, with the start of a full-scale war in Ukraine. However, in Georgia, Russia uses influence operations, which are different from warfare and are relatively unnoticeable, yet very active. Since Russia sees Western democracies as the main threat and its task is to limit the enlargement and influence of the European Union and NATO, the active use of influence operations in Georgia will stop the strengthening of these organizations.

In Russian strategic thinking, main actor is Russia, which actively uses hybrid methods and spheres of influence to blur the line between war and peace. Thereby, it fulfills its own interests. Russia sees the U.S., EU and NATO as attacker actors. The secondary actors are the post-Soviet countries of the wider Black Sea region that have the desire and the chance to join the EU and NATO. Specifically, Georgia, Ukraine and Moldova. i

Russia's active use of hybrid methods in Georgia is manifested both in the use of soft power, such as propaganda, disinformation, active use of trolls and bots and influence on public opinion. As well as in more difficult and complex steps, such as the so-called borderization, cyberattacks, increasing economic dependence, active intervention in Georgia's internal and foreign affairs, and giving instructions on what Georgia must diio.

Russia's hybrid methods in the wider Black Sea region, and in particular in Georgia, are quite damaging. However, this problem and challenge do not concern only Georgia. The war waged in Ukraine and the punishment of Georgia for its pro-European course are not local and ordinary challenges for Europe. Quite the opposite, Russia's use of hybrid methods in the wider Black Sea region poses a significant threat to European security. Obviously, if the EU and especially NATO are defeated in Ukraine, then Russia will strengthen its positions and move to other European and post-Soviet countries with aggression and possible war. For Russia, it is necessary that Georgia remains alone, without Western protection and security guarantees. Western

aid and support ensures Russia's containment and weakening in the wider Black Sea region, which Russia considers important for its security. Clearly, the protection of this region and Georgia in particular, is essential for the security of Western organizations.

Information warfare methods used by Russia in Georgia from the invasion of Ukraine to Georgia's November 28 statement

International security has changed since Russia invaded Ukraine on February 24, 2022. Simultaneously, since Russia's invasion of Ukraine, the narrative of the ruling party in Georiiigia, the Georgian Dream, has been changing towards a negative one in relation to Western countries, organizations and Ukraine. This was particularly evident in the statement of November 28, 2024, when the Prime Minister with questionable legitimacy, Irakli Kobakhidze, announced the suspension of Georgia's negotiations with the European Union until 2028. Obviously, Russia actively contributed to the creation of the tense environment and the weakening of the EU/NATO so that it would not lose its influence in Georgivia during the war in Ukraine. To do this, Russia used information warfare methods, which are mainly aimed at social media and its users. It is often very difficult to filter information on social media, especially for people who do not check the factual accuracy of information or do not have sufficient knowledge of foreign languages to check it in foreign media outlets. Accordingly, such people become vulnerable to Russian information warfare methods. v

In parallel with the war in Ukraine, Russia's information warfare methods in Georgia such as propaganda, disinformation and trolls/bots, have become even more powerful and active. Russia's main focus is on managing social media and spreading disinformation that appeals to the sensitive side of society. The main participants in this strategy are pro-Russian and anti-European media outlets, such as TV Imedi, POSTV and other small media companies that mainly operate in social networks. Russia, through propaganda and the creation of a false image spread by trolls and bots, stirs up anti-EU and NATO sentiments, forms erroneous views and thus tries to take Georgia away from the Western course. Obviously, Putin's main interest now is that in parallel with the war in Ukraine, a negative attitude towards Russia does not arise. Most importantly, those measures will stop NATO to enlarge. Since Putin has already lost Finland, he will continue to do so through military aggression in Ukraine, active political intervention in Moldova and information warfare in Georgia, to completely remove NATO and the European Union from the foreign policy of these countries.

Moreover, Russia uses borderization to spread disinformation against NATO. It presents the North Atlantic Treaty Organization as incapable, lacking the power to resolve the conflict. In addition, the Kremlin spreads disinformation that NATO requires Georgia to recognize the occupied territories as states in order to join in it. Such a narrative significantly damages the reputation of European organizations in Georgia. Also, Russia spreads the idea that Georgia's NATO membership will lead to war with Russia.

Non-governmental organization, ISFED investigated the issue of pro-Russian propaganda in Georgia against the European Union since 2022. The investigation traced fake accounts that were created in Russia and included various social media networks – Facebook, Instagram, TikTok, Telegram. The network of these accounts wrote posts with identical content in the local languages in Georgia, Armenia and Azerbaijan. The network of fake accounts operated from Russia actively supported "Georgian Dream" and used disinformation to create contrasting images. As an example, the ruling party is presented as a defender of religious, traditional family values and national interests, while on the other side is an European politician whose sexual orientation is used by Russia to harm the reputation of European Union. Obviously, for a country with such traditional views as Georgia, such simple propaganda has an effect on certain segment of society. As a result, skepticism toward the European Union and NATO is growing, which is Russia's direct interest and perfectly fulfills the task of Russian information warfare methods.

The significance of Russian influence operations in Georgia for the wider Black Sea region

The success of influence operations directed at Georgia significantly weakens any region that includes Georgia. If Russia manages to become a dominant power in the wider Black Sea region, this will be a major geopolitical and security challenge for the EU and NATO. Therefore, Russia's influence operations in Georgia are very dangerous.[vii]

As Russia's influence in various regions has shifted negatively, Georgia has become a battleground where Russia is trying to consolidate its position. For example, in Caucasus region, where Kharabakh conflict between Armenia and Azerbaijan ended with a peace treaty with[viii]the active involvement of the United States and European states, relations between the two countries have normalized. Russia is no longer a

relevant and major power. In parallel with this development, Russia failed to fulfill its obligations to Armenia within the frameixwork of the Collective Security Treaty Organization, which led to a strained relationship between Armenia and Russia. "The OAS has not fulfilled its security obligations towards Armenia, especially in 2021 and 2022. This cannot go without consequences. The result is that in practice we have basically frozen our participation in the OAS," said the Prime Minister of Armenia, Nikol Pashinyan. Armenia's choice of Western course and the adoption by the parliament of a bill by a majority vote that should ensure Armenia's accession to the European Union is radically different from Georgia's current course, which leans towards Russia. Accordingly, now the main stronghold for Russia in the Caucasus region is Georgia, where Russian influence operations are successful.

The Caucasus region is connected to the Middle East. Here, too, Russian influence weakened when the Russian-backed Assad regime in Syria ended. Syria became a country with a multi-vector foreign policy, which now includes cooperation with the EU and NATO member states. The Russian bases in Syria on the Mediterranean Sea and the existence of Russian bases is also questionable. While Russia suffered colossal losses in the war with Ukraine, with the sinking and destruction of its Black Sea Fleet, it is also losing the Mediterranean Sea. These issues concern not only the military sphere, but also energy security and oil. Accordingly, Russia's influence in the Middle East ixs decreasing.

Overall, the wider Black Sea region is at the crossroads of the South Caucasus, the Middle East and the Balkans, including Georgia, an important actor for Russia. As its influence gradually diminishes, the implementation of influence operations against Georgia's Western course stirs up Russian narratives, skepticism towards Western democracies, specifically targeting the EU and NATO. Funded propaganda spread by hired trolls and bots, disinformation that mixes reality and falsehood – all of them help Russia maintain its influence in Georgia. This is especially alarming for the West, for whose security it is vital to stop Russian influence in the wider Black Sea region. Especially when a full-scale war is already underway here. However, it is not a good thing for Russia either. Russia is actively being weakened by Ukraine in the Black Sea region while Putin is unable to achieve significant success in the war. All this further facilitated by Georgia's recent political decisions, the postponement of negotiations with the European Union and the artificial straining of relations with West. Overall, all of the above-mentioned steps create a perfect space for Russia to maintain its influence

in the Wider Black Sea region through Georgia, when in many countries Putin lost the power. As a result, NATO and EU, perceived as a hybrid threat to Russia, face a significant challenge.

What can the EU and NATO do to stop the success of Russian influence operations in Georgia?

For Western democracies, Russian influence operations in Georgia are a real threat. I believe efforts of the EU and NATO to counter Russian disinformation and propaganda are not enough. For an ordinary citizen who receives information from social media and may naively believe a lie, it is unclear how Georgia's accession to the EU and NATO will improve their well-being, standard of living and security in general. This problem has become especially evident after the Georgian Dream Party began to actively criticize European democracies, thereby fueling Euroscepticism. They started to appeal to the issue of war and peace, as if Georgia's European integration would start war with Russia. As I have already mentioned, strong and vast Black Sea region free from Russian influence is a guarantee of European security. However, I believe that European countries still need to be more active in this regard.

- Georgian territories are occupied by Russia and citizens are vulnerable to Russian propaganda, it is important to stabilize political environment and individuals who contribute to undermine democracy must be sanctioned.
- In terms of protecting human rights, patrolling the illegal border should be strengthened and NATO must ensure that the security of every citizen of Georgia is protected.
- It is important to strengthen campaigns that provide the population living outside the capital with correct, official information about the activities of the EU/NATO and their benefits. This will make it difficult for Russian propaganda to easily convince Georgian people.
- It is necessary to constantly monitor social media and actively communicate with META regarding suspicious accounts.

I think that in these ways the West will be able to weaken Russian influence in Georgia, which will significantly weaken Russia's positioning in the wider Black Sea region.

CONCLUSION

Russia's active use of influence operations contribute to achieving its strategic objectives, which include weakening the EU and NATO in states it perceives as spheres of influence. Georgia is an important country not only in this context, but also in the wider Black Sea region. While Putin becomes weaker in every other region, he tries to maintain Russian power in Georgia.

Since 2022, Russia has further intensified its influence operations in countries perceived as its sphere of influence. Especially in Georgia, where the Georgian Dream party and the Kremlin share identical political thoughts.

Thus, ruling party follows Russian footsteps and copies Russian laws, narratives and propaganda. By strengthening Russian influence in the wider Black Sea region, Russia has captured an important space - Georgia. This is major challenge and problem for the security of the European Union and NATO. In the future, Russia's influence operations might become even more aggressive, direct and dangerous. Now it is on West to be more active and adaptable towards Russian hybrid threats and to protect free nations threatened by Russia, especially Georgia.

Photo: Occupation Line in Khurvleti, Georgia. Shutterstock

[i] Sikharulidze, V. (2025). Russian Influence Operations in Georgia: A threat to Democracy and Regional Stability. Foreign Policy Research Institute. https://www.fpri.org/article/2025/03/russian-influence-operations-in-georgia-a-threat-to-democracy-and-regional-stability/.

[ii] Benia, M. (2025). *As Georgia dismantles its civil service, the Kremlin watches and wins.* New Eastern Europe. https://neweasterneurope.eu/2025/08/25/as-georgia-dismantles-its-civil-service-the-kremlin-watches-and-wins/.

[iii] Sikharulidze, V. (2025). Russian Influence Operations in Georgia: A threat to Democracy and Regional Stability. Foreign Policy Research Institute. https://www.fpri.org/article/2025/03/russian-influence-operations-in-georgia-a-threat-to-democracy-and-regional-stability/.

[iv] Russian information operation in Georgia supporting the ruling party and discrediting the EU. ISFED. (2024). https://isfed.ge/eng/sotsialuri-mediis-monitoringi/rusuli-sainformatsio-operatsia-saqartveloshi-mmartveli-partiis-sasargeblod-da-evrokavshiris-tsinaaghmdeg.

[v] Seskuria, N. (2021). Russia's "Hybrid Aggression" against Georgia: The Use of Local and External Tools. Center for Strategic & International Studies. https://www.csis.org/analysis/russias-hybrid-aggression-against-georgia-use-local-and-external-tools.

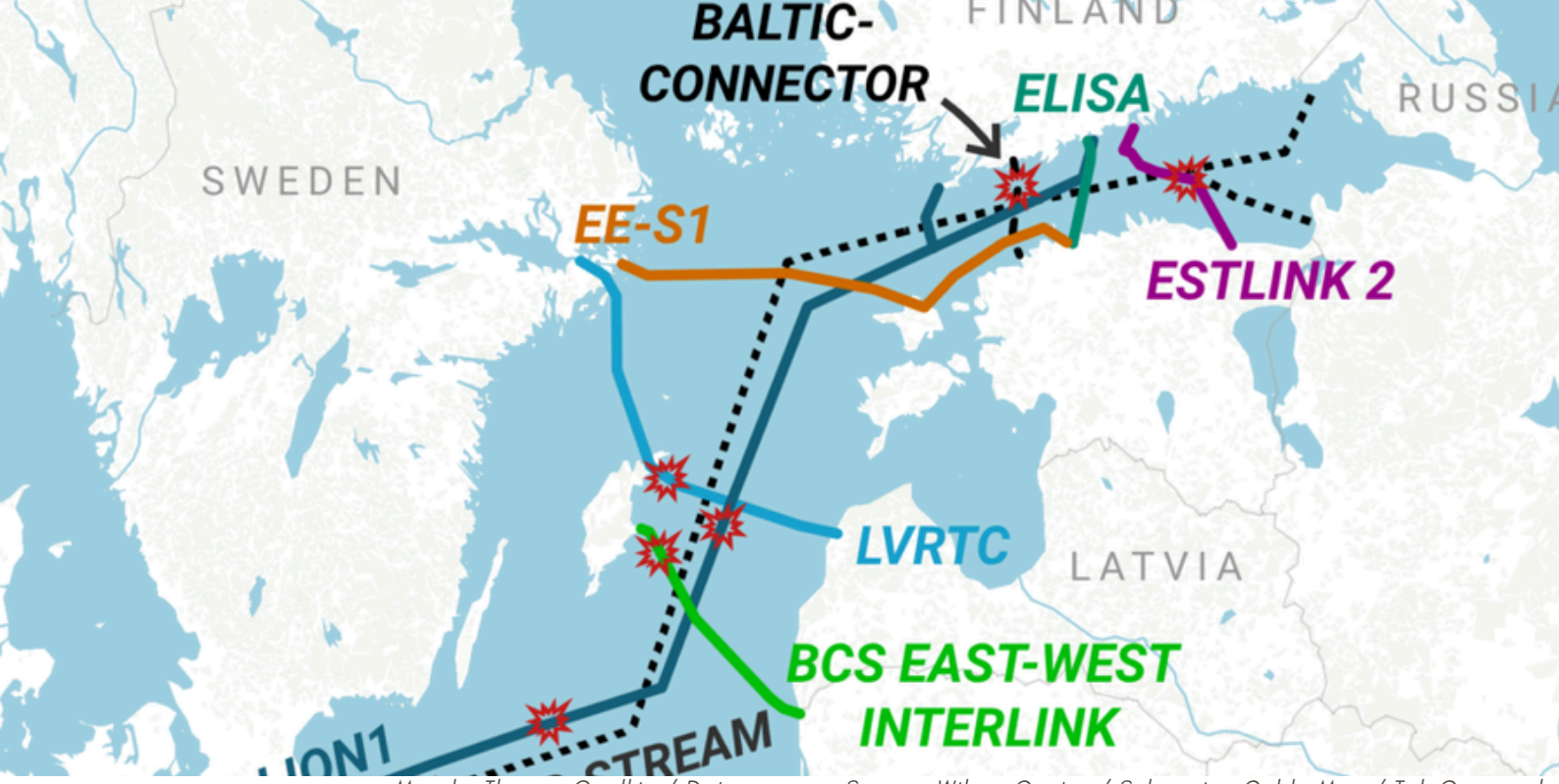
[vi] *ფაშინიანი: სომხეთის მონაწილეობა ОДКБ-ში პრაქტიკულად გაყინულია.* (2024). პუბლიკა. https://publika.ge/fashiniani-somkhetis-monawileoba-%d0%be%d0%b4%d0%ba%d0%b1-shi-praqtikulad-gayinulia/.

[vii] *ევროკავშირი აქებს სომხეთთან ურთიერთობების გაღრმავების „უპრეცედენტო ტემპს".* (2025). რადიო თავისუფლება. https://www.radiotavisupleba.ge/a/33415193.html.

[viii] Notte, H. (2025). Russia Isn't Done With Syria - How Moscow Has Retained Influence in the Post-Assad Era. Foreign Affairs. https://www.foreignaffairs.com/russia/russia-isnt-done-syria.

[ix] Benia, M. (2025). As Georgia dismantles its civil service, the Kremlin watches and wins. New Eastern Europe. https://neweasterneurope.eu/2025/08/25/as-georgia-dismantles-its-civil-service-the-kremlin-watches-and-wins/.

[x] Sabanadze, N. Dalay, G. (2025). Understanding Russia's Black Sea strategy. Chatham House. https://www.chathamhouse.org/2025/07/understanding-russias-black-sea-strategy/02-russias-use-conflicts-black-sea-region.



Map by Thomas Gaulkin / Datawrapper; Source: Wilson Center / Submarine Cable Map / TeleGeography

Ketevan Ioseliani

Democratic Deterrence in the Gray Zone: NATO and Critical Undersea Infrastructure in the Baltic Sea

Liberal democracies are inherently shaped by law. This, in turn, has costs that appear under heightened security pressure - a democratic state that has bound itself to law cannot unbind itself as easily or selectively whenever it wants to. A democratic state needs a response that is effective yet proportionate and requires measures that satisfy democratic requirements to the fullest extent possible. Therein, the undersea infrastructure is one domain where those costs are now being paid.

Ninety-nine percent of inter-continental internet traffic is carried by submarine communication cables. These interconnectors tie national grids together, and their disruption may lead to repercussions that exceed regular physical damage alone. Against this backdrop, and after recognizing the likely outcomes, NATO has been building continuously robust operational tools to "deter, detect and respond to threats" against them. This, in itself, indicates that the issue should be sought and discovered outside NATO's operational capabilities, especially in the gap that exists between what evidence demonstrates and what a criminal court threshold ultimately requires. Deterrence that depends on the final verdict of the prosecution works on a timescale that is too slow and, in turn, gives the strategic, asymmetric edge to the adversary. Therefore, NATO and its Allies demand mechanisms that respond to the observable conduct and do not require conclusive proof of hostile intent, which causes relative delays during the decision-making process.

Critical Undersea Infrastructure in the Gray Zone

"Hybrid war is truly 'war' in a Clausewitzian sense," [i]and since NATO is not an official party to Russia's war in Ukraine, the concept of gray-zone more accurately describes sabotage activities, and especially damage to CUI. It maneuvers "in the ambiguous no-man's-land between peace and war…but without the overt use of military force."[ii] Mazarr describes it as the efforts that "remain below threshold."[iii] Because of this ambiguity, NATO has no grounds to automatically treat such incidents as acts of war, and this alone limits the scope and full capability to respond effectively when it is deemed necessary.

It follows that Russia's shadow fleet operates within this gray zone. Estimates put the total vessel count range at 1,000 to 3,200 (the Ukrainian government puts the number at 1,392). Those identified vessels operate through flags of convenience, shell-company ownership, name changes, AIS manipulation, and, in addition, open sources associate them with undersea cable incidents, yet attribution continues to be a main predicament[iv] and can be described as "asymmetric weapon(s) to achieve geopolitical objectives"[v]. From this comes a simple truth that a hostile actor need not rely on specialized sabotage vessels when an ordinary one can simultaneously provide a way, functional cover, and strategic ambiguity, all the characteristics that give the asymmetric advantage to one side within the gray zone.

That ambiguity creates a dilemma for liberal democracies. The question arises and asks if a response that nobody hears send any signal of deterrence? The answer is simply no. And if it does not, it can not indeed deter anyone[vi]". Hence, a visible response is required, but ambiguity turns every visible response into a legal test, and that legal test begins with jurisdiction. UN Convention on the Law of the Sea (UNCLOS), Article 113, obliges states to criminalize damage to submarine cables by their ships when "done wilfully or through culpable negligence."[vii] Article 97 of the same document reserves penal proceedings for an "incident of navigation" to the "flag State or of the state of which such person is a national."[viii] Only a small number of states have in reality implemented Article 113, and a victim state that faces an inactive flag is left with inter-state arbitration, "strategic litigation," which gives us no "definite answer."[ix]. Coastal states, in turn, do have the possibility and the right to extend jurisdiction (based on the effects doctrine and the protective principle), but this route concerns deliberate

damage,[x] therefore, the main and most promising jurisdictional route depends on the ability to prove that the damage done was not an incident.

From Detection to Deterrence: The Attribution Gap

Over time, NATO's undersea capabilities have matured, which has been borne out particularly by developments between 2023 and 2024, when the Alliance established the CUI Infrastructure Coordination Cell and Maritime Centre for the Security of CUI. This continued in 2025, when Baltic Sentry was launched[xi]. In addition, Task Force X-Baltic has shown persistent surveillance through the deployment of air, surface, and subsurface systems and has monitored vessels on a daily basis, among them Russian shadow-fleet and military assets[xii]. What this reveals is that for NATO, surveillance is not an impediment, and we should search and identify the problem elsewhere.

At the initial stage, particular attention must be given to the Yi Peng 3 case, which shows off the distinction between the detection of an incident and the establishment of a real, substantive intent. The Swedes were able to reconstruct the anchor drag in precise detail[xiii], but Chinese control of the vessel constrained access, after which the Swedes could not conduct interviews with those on board[xiv]. In the end, Yi Peng 3 shows that surveillance can indeed identify the damage, but when it comes to finding evidence, the measures, in certain circumstances, fail, and the flag state holds the key.

Another case identifies the same problem pointedly, with more precision. That is Eagle S Tanker, built in China, flagged in the Cook Islands, managed by Caravella LLC, a UAE-registered company, with the Azerbaijani businesswoman as a legal owner (though she denied it)[xv], and the captain, on the other hand, a Georgian citizen[xvi]. These jurisdictions, which clearly overlap and include multiple possible attributions, further complicate the real attribution process and make it clear why claiming specific state involvement remains a particular challenge. When Finland seized the ship, the Helsinki District Court found that it had no legal power to do so (under UNCLOS). Soon after, Finland appealed (yet the process has not been finalized), and it indeed restored the prosecution process, but what, in turn, could not be restored was several months and three officers who had already left the country[xvii]. Accordingly, the central problem that democracies face when they have to act real quick is that the establishment and demonstration of legal basis for that exact action takes time, which might leave past efforts in vain.

Herein, the asymmetry is institutional, and a democracy must prove intent to a criminal standard against the same opponent who carefully worked, meticulously designed and planned each incident to appear accidental. Those cases show us an important inference that mere detection does not provide us with the evidence required to establish intent or the legal authority, especially while operating within the gray zone. Nye, writing about cyberspace, where attribution is similarly difficult, identified that the latter is particularly relevant to punishment, and is one of four mechanisms of deterrence, alongside denial, entanglement and normative taboos.[xviii] Compared to the cyber domain, CUI punishment runs through different jurisdictions, different processes such as boarding, seizure, prosecution, and may also be subject to appellate review - hence, it takes time, has many layers, and when legal grounds for punishment are complete, the strategic opportunity for deterrence may have already passed.

Recommendations

- **Make rapid recovery part of NATO's deterrence strategy** - Estlink 2 took several months to repair and demonstrated the lengthy, resource-intensive nature of subsea cable repair.[xix] As NATO already has a robust infrastructure, the key here is to maintain a resilient and persistent naval presence so the damaged cables can be repaired as quickly as operationally feasible, ideally within days. This recommendation depends on the joint action between the Allies, the EU, and operators investing in repair vessels. Following this recommendation, the sabotage will most likely fail to achieve its intended impact, as this will create fewer strategic gains for the adversaries (that is Nye's deterrence by denial, which can operate without definitive attribution[xx]). The cost, however, falls mainly on national budgets and operators.
- **Impose lawful costs before criminal cases are concluded** - Entirely dependent on collaboration between NATO and the EU, and their joint efforts, where both would strengthen existing economic and administrative measures against vessels that are linked to incidents, where the law allows. Although it must be regarded as a complementary proposal (not a replacement) to criminal proceedings to ensure that deterrence does not depend only on a final conviction, which may take years or may never be finalized. The identified cost here is escalation and the risk to penalize an innocent people due to quick attribution. This must be avoided at all costs, and it is relatively easy to do so.

- **Set clear rules just for the Baltic Sea** - NATO should make it possible to pre-approve and agree in advance on how to respond and what action is legally possible when CUI is damaged, especially when it comes to the Baltic Sea area, the most sensitive in that regard. This, in itself, would make response faster, with no costs and without giving NATO unlimited powers and removing the judicial oversight
- **Improve communication between NATO and national authorities** - Immediately after damage to CUI is detected, a relatively faster system for information sharing is required, which will allow data and evidence to reach national authorities faster, so that the states can first decide which legal or economic action to take. It is proposed entirely to prevent delays between detection and response and would give practical meaning to the commitment of the Alliance Maritime Strategy to attribute incidents[xxi]. Although some material will stay classified to protect sources, and not everything NATO has information on will be unfolded inside a courtroom.

CONCLUSION

Drawing on the previous analysis, NATO's structural predicament is not operational, and surveillance, detection, and military security are not the obstacles that the alliance needs to surmount - those are instead among NATO's more robust capabilities. What continues to pose a concern is the handling and resolution of institutional and legal lags that emerge thereafter. It is the exact structural problems that adversarial actors actively capitalize on by exploiting the inherent characteristics of democratic systems and weaponizing due process into their own strategic advantage. These structural problems should not be interpreted as requiring NATO or any other relevant democratic states to compromise their standards or discard judicial/legal accountability. However, deterrence among the allies must not rest entirely upon reaching the final stage of attribution. The aforementioned recommendations of this paper would equip the Alliance and allies to respond to the strategic problem that poses an immediate threat whilst also upholding already extant legal processes. This, in turn, carries a broader lesson that uncertainty should not become a reason for inaction. Seen in these terms, protecting CUI would reflect the wider remit of the alliance - to be prepared to "fight tonight" and "fight tomorrow".

Photo: Navy ships sail during the Northern Coasts 2023 exercise in the Baltic Sea, September 18, 2023. REUTERS/Janis Laizans

[i] Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2015), 62, https://press.armywarcollege.edu/monographs/428
[ii] Mazarr, *Mastering the Gray Zone*, 17
[iii] Mazarr, *Mastering the Gray Zone*, 16
[iv] Armed Conflict Location&Event Data Project (ACLED), "Russia's Shadow Fleet Presents a Sustained Hybrid War Threat at Sea," 2026, ACLED, https://acleddata.com/report/russias-shadow-fleet-presents-sustained-hybrid-war-threat-sea
[v] Moritz Brake, "Russia's Shadow Fleet as an 'Asymmetric Weapon' in Hybrid Warfare," CASSIS – Center for Advanced Security, Strategic and Integration Studies, University of Bonn, January 11, 2025, https://www.cassis.uni-bonn.de/en/media-contributions/brake-russland-schattenflotte
[vi] Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 2008), 55.
[vii] United Nations, *United Nations Convention on the Law of the Sea*, December 10, 1982, 1833 U.N.T.S. 397, art. 113, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf
[viii] United Nations, *United Nations Convention on the Law of the Sea*, art. 97.
[ix] Lott, Alexander. "Conventional Jurisdictional Approaches to Protecting Submarine Cables and Pipelines." *International and Comparative Law Quarterly* 74, no. S1 (2025): 71. https://doi.org/10.1017/S0020589325101164.
[x] Lott, "Conventional Jurisdictional Approaches," 63,71.
[xi] NATO, "NATO's maritime activities," updated 10 March 2025. https://www.nato.int/en/what-we-do/operations-and-missions/natos-maritime-activities
[xii] NATO Allied Command Transformation, "Task Force X-Baltic," especially the June 2025 demonstration. https://www.act.nato.int/activities/tfx-b/
[xiii] Reuters, "Swedish probe finds no conclusive evidence of deliberate cable damage by Chinese ship," April 15, 2025. https://www.reuters.com/world/europe/swedish-probe-finds-no-conclusive-evidence-deliberate-cable-damage-by-chinese-2025-04-15/
[xiv] Reuters, "Swedish probe finds no conclusive evidence of deliberate cable damage by Chinese ship."
[xv] Yle News, "Don't disturb me," says Azerbaijani Eagle S owner," August 29, 2025. https://yle.fi/a/74-20180061
[xvi] Reuters, "Tanker captain accused of Baltic cable cut tells Finland's YLE he is 'innocent'," August 22, 2025. https://www.reuters.com/business/media-telecom/tanker-captain-accused-baltic-cable-cut-tells-finlands-yle-he-is-innocent-2025-08-22/
[xvii] "Prosecutor appeals judgement in the Eagle S case," Finnish Prosecution Service, Finnish Government, October 9, 2025, https://valtioneuvosto.fi/en/-/11121156/prosecutor-appeals-judgement-in-the-eagle-s-case
[xviii] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/17): 54-55, 60-61. https://doi.org/10.1162/ISEC_a_00266
[xix] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, *"Joint Communication to the European Parliament and the Council: ProtectEU-A European Internal Security Strategy,"* JOIN(2025) 9 final, February 21, 2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025JC0009
[xx] Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace"
[xxi] NATO Allied Command Transformation. "NATO's Mainsail: Enhancing the Security of Critical Undersea Infrastructure through Advanced Data Exploitation." January 21, 2025. https://www.act.nato.int/article/natos-mainsail/

Photo: Election Day in the U.S., November 5, 2024. REUTERS/Quinn Glabicki

Ana Javakhishvili

Russian Influence Operations Against the United States During the 2016 and 2024 Presidential Elections

Russia's strategic approach increasingly relies on hybrid threats that combine cyber operations, foreign disinformation, artificial intelligence (AI), and psychological manipulation to weaken democratic institutions and expand Moscow's influence. Comparing Russian influence operations during the 2016 and 2024 U.S. presidential elections reveals a clear evolution in operational capabilities. Whereas the 2016 campaign relied heavily on social media manipulation to amplify existing societal divisions, the 2024 campaign incorporated more advanced technological tools, including AI-generated content, deepfakes, and automated bot networks.

To address this evolving threat, the United States should move beyond primarily reactive countermeasures toward a more proactive and integrated policy framework. Priority measures include establishing real-time threat-information-sharing mechanisms among intelligence and law-enforcement agencies and technology platforms, introducing provenance and disclosure standards for AI-generated political content, and strengthening public resilience to foreign information manipulation.

Russian Influence Operations as a Hybrid Threat to Democratic Governance

Russia's strategic policy treats the United States and democratic alliances as major geopolitical adversaries. Moscow therefore employs unconventional warfare and hybrid methods to disrupt governance, erode public trust, and exploit the openness of democratic information environments while remaining below the threshold of direct military conflict. Rapid advances in generative AI and automated digital media have further reduced the cost and increased the potential reach of high-impact foreign influence operations.

This paper asks: How do Russian influence operations against the United States undermine Western democratic values and governance structures, and what strategic policy framework is needed to mitigate these evolving hybrid threats?

From Soviet Active Measures to Contemporary Influence Operations

Russia has a long strategic tradition of unconventional warfare rooted in practices developed during the Soviet era. During the Cold War, the USSR conducted extensive campaigns designed to influence foreign audiences, expand Soviet influence, and weaken U.S. institutions and principles—activities that became known as "active measures." Under the direction of Soviet intelligence services, particularly the KGB, these measures included disinformation and "gray" and "black" propaganda, the use of foreign agents of influence, clandestine radio broadcasting, support for revolutionary and terrorist organizations and national liberation movements, political blackmail, and kidnapping. The United States was a principal target, while Soviet operations in Europe also sought to fracture the Euro-Atlantic alliance and diminish U.S. influence abroad.[i]

Russia's 2016 Campaign: Exploiting Democratic Vulnerabilities

During the 2016 election, Russian influence operations sought to shape the American electorate's perceptions and weaken trust in democratic processes through a combination of digital and other influence tactics. Russian disinformation targeted actors across the political spectrum, including Republican Senators Marco Rubio and Ted Cruz, Black Lives Matter activists, and separatist movements in Texas and California. The broader objective was to intensify existing polarization in the United States and destabilize confidence in the democratic and electoral process.[ii]

Social media platforms, particularly Facebook and Twitter, were central to these operations. Russian actors created deceptive accounts, deployed troll and bot networks, and purchased advertisements designed to inflame racial, class, ideological, and social tensions. Content was also used to provoke confrontation between groups with opposing political views, thereby exploiting existing divisions within American society.[iii]

In 2018, the FBI announced that 12 Russian military intelligence officers had been indicted by a federal grand jury in the District of Columbia for alleged interference in the 2016 presidential election. Eleven were charged in connection with a hacking conspiracy involving unauthorized access to computers belonging to U.S. individuals and organizations. Two were additionally charged in a separate conspiracy involving intrusions into systems associated with U.S. election boards, companies, and state election authorities.[iv]

The 2024 Election: From Disinformation to AI-Enabled Influence

Two months before the 2024 election, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated ten individuals and two entities as part of a coordinated U.S. government response to Moscow's efforts to exert malign influence over the presidential election. Russian state-linked actors increasingly incorporated artificial intelligence, deepfake content, and disinformation into influence operations targeting U.S. electoral processes. In early 2024, leaders of the Russian state-run media outlet RT also sought to recruit unwitting Americans to support Russian influence activities.[v]

The FBI also warned about fabricated videos and statements circulating online that misused the agency's name and insignia to promote false election-related narratives. Although the FBI did not attribute those materials to a specific foreign state, researchers cited in contemporaneous reporting assessed that they were likely connected to Russian influence operations.[vi]

Recommendations

1. Counter-Disinformation and Interagency Coordination

- Establish rapid, legally governed information-sharing mechanisms among the Department of Homeland Security, the FBI, other relevant agencies, and major

technology platforms to identify and disrupt foreign influence accounts and coordinated bot networks.

- Continue using targeted Treasury Department sanctions and financial-disruption measures against foreign actors and entities that finance or facilitate disinformation and covert online influence operations.

2. Regulatory and Technological Safeguards

- Develop technology-neutral rules requiring providers of generative AI systems to support reliable provenance mechanisms—such as metadata, watermarking, or other forms of content authentication—for AI-generated images, audio, and video used in political contexts.
- Require online platforms to provide clear, proportionate disclosures when accounts are controlled by foreign state actors, substantially automated, or distributing AI-generated political media, while ensuring that enforcement standards are transparent and subject to appropriate oversight.

3. Public Resilience and Election Security

- Expand public media- and information-literacy initiatives that help citizens identify disinformation, manipulated media, impersonation, and other common influence techniques.
- Increase federal support for state and local election authorities to assess vulnerabilities, secure voter-registration and election-related digital systems, and strengthen defenses against foreign cyber intrusions.

CONCLUSION

Russian influence operations during the 2016 and 2024 U.S. presidential elections demonstrate an evolution in Moscow's use of hybrid methods. These operations combine disinformation, cyber capabilities, and psychological influence to erode trust in democratic institutions, exploit social divisions, and weaken Western cohesion without relying on direct military confrontation.

This approach reflects a broader preference for pursuing strategic objectives through instruments that remain below the threshold of conventional conflict, particularly in competition with the United States and its allies.

Hybrid threats therefore remain an important component of Russian strategic thinking and a persistent challenge for democratic states. The evolution of influence operations also highlights the vulnerabilities created by open information environments, rapid technological change, and fragmented institutional responses.

Mitigating these risks requires a comprehensive policy approach that combines regulatory safeguards, interagency coordination, election-system security, financial disruption of malign actors, and sustained investment in public resilience.

Photo: Illustration taken in Moscow on November 10, 2016. Russian newspapers reporting on after the US presidential election. YURI KADOBNOV/AFP/Getty Images

[i] Seth G. Jones, "Russia's Shadow War Against the West," Center for Strategic & International Studies, March 2025, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-03/250318_Jones_Russia_Shadow.pdf?VersionId=LHamL2L7HGwLgZ7a_wq6xkTIwMh3TFpk

[ii] Security Alliance, "Changing Ballots and Minds: Russian Influence Operations and the 2024 U.S. Presidential Election," November 7, 2024, https://www.secalliance.com/blog/changing-ballots-and-minds-russian-influence-operations-and-the-2024-us-presidential-election.

[iii] Nicola Mlinac, "Hybrid Intelligence as a Carrier of Disinformation and Hybrid Threats in Cyberspace," National Security and the Future 26, no. 1 (2025): 65–98, https://www.nsf-journal.hr/Portals/0/Dokumenti/Volume26,%20No1%202025/005-NSF-2025-No%201%20-%20vol%2026%20-%20Mlinac%20-%20065-098%20.pdf.

[iv] U.S. Federal Bureau of Investigation, "Russian Interference in 2016 U.S. Elections," accessed March 2026, https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections.

[v] U.S. Department of the Treasury, Office of Foreign Assets Control, "Treasury Takes Action as Part of a U.S. Government Response to Russia's Foreign Malign Influence Operations," press release, September 4, 2024, https://home.treasury.gov/news/press-releases/jy2559.

[vi] Huo Jingnan, "Foreign-Influence Efforts Reached a Fever Pitch During the 2024 Elections," NPR, November 9, 2024, https://www.npr.org/2024/11/09/nx-s1-5181965/2024-election-foreign-influence-russia-china-iran

Photo: Alaska Summit, Aug. 15, 2025.AP Photo/Julia Demaree Nikhinsoni

Luka Beridze

Appeasing Russia: The Escalation of the Kremlin's Aggressive Policy and the Failure of Western Soft Deterrence

After the Cold War, Western expectations regarding Russia proved false, and the Kremlin gradually became one of the biggest threats to the contemporary international security system. While the European Union and the U.S. tried to normalize relations with [i]Moscow, Russia returned to direct military aggression in its neighborhood—for example, by attacking Georgia in 2008 and Ukraine in 2014, annexing Crimea, and backing separatism in the Donbas. Later, Russia intervened in the Syrian civil war, where the Kremlin supported Bashar al-Assad's regime. Through these actions, Russia advanced its geopolitical and economic interests.

Russia's aggression against Georgia in 2008 did not trigger any real response from[ii]the EU or the U.S.. Just three months after the war, an EU summit concluded that economic relations with the Kremlin remained consistent and that this trend should continue.

As a result, by 2021, trade between the EU and Moscow exceeded 240 billion euros. Meanwhile, just a few months after his inauguration, U.S. President Barack Obama announced a "reset" policy with Russia and shifted Washington's strategic focus to Asia. This decision left Eastern Europe vulnerable to Russian threats, and the Kremlin took advantage of the resulting power vacuum.

After establishing a precedent of impunity in the post-Soviet space, Moscow expanded its influence into the Middle East as well. Russia intervened in the Syrian civil war, seizing a solid opportunity for geopolitical and economic gains. The US was entirely focused on anti-ISIS operations and had no plans to confront Russia's involvement.

The research question of this paper is: "What impact did the West's passive policy have on the expansion of Russia's spheres of influence?"

Signals of Russia's Aggressive Policy

In this chapter, we will discuss signals from Russia's internal and foreign policy that were ignored by Western countries.

Political Repressions and Authoritarianism

Shortly after assuming the presidency, Vladimir Putin began consolidating his power through media censorship, the imprisonment of political opponents, and the murder of journalists.i

A particularly high-profile case was the 2006 murder of Anna Politkovskaya, Putin's most prominent journalistic critic. Her assassination served as a clear warning to all other opposition journalists, as highlighted by Alexei Simonov, head of the Glasnost Defense Foundation: "The effect of Anna's murder is simple—now every journalist will censor themselves and think three times before writing anything".

The rise of authoritarianism, political murders, and the destruction of civil society should have been a signal for Western countries that their optimism regarding Moscow was false. Despite this, the West continued its partnership policy with Russia.

Munich Speech

Vladimir Putin's 2007 speech at the Munich Conference dispelled any doubts regarding the Kremlin's positions.ii

Putin used the Color Revolutions in Georgia and Ukraine as one of the main precursors to his speech. A core theme of the Munich address was the concept of "Great Power status" (*Derzhavnost*)—the idea that Russia, as a historically great power, is entitled to its own spheres of influence. Putin also challenged the hegemony of the United States and criticized the unipolar international order, effectively signaling a strategic confrontation with Washington. The president openly stated that if the world refused to consider Russia's interests, he was ready to defend them by force.

Based on all this, Putin's Munich speech was essentially an announcement of his future strategy: the fight for spheres of influence. However, instead of taking the threat from Moscow seriously and working on containment, the European Union deepened its economic ties with Russia. Shortly after, the new White House administration announced a "reset" policy with the Kremlin.

The 2008 Georgia War

The 2008 NATO Bucharest Summit had a major influence on Russia's decision to attack Georgia. NATO decided not to grant a Membership Action Plan (MAP) to Georgia and Ukraine; instead, they included a vague clause: "NATO welcomes the Euro-Atlantic aspirations of Georgia and Ukraine. We have agreed that these countries will become NATO members."

Even after the war, the IIFFMCG (also known as the Tagliavini Report) reached ambiguous conclusions about who started the conflict. Western countries viewed Georgia's case as an exception—an isolated event rather than the first iiisign of a systematic threat. The West shared the responsibility for starting the war between both countries and soon normalized relations with the Kremlin, returning to "business as usual."

Despite the Georgian war, the EU deepened its economic ties with Russia. From 2008 to 2014, the share of Russian natural gas in the EU market increased from 31% to 37%, whileivfor oil, Moscow remained the main supplier (30–34%). A standout example is the Nord Stream 1 project between Germany and Russia, which provided Russia with economic profit and political leverage. In addition, Nord Stream 1 reduced the transit significance of Eastern European countries, such as Poland and Ukraine. Germany's *Wandel durch Handel* (stable peace based on economic integration) policy was a complete failure—economic integration did not guarantee peace, but led to destabilization instead.

Europe's defense policy is another clear indicator of how the Russian threat was disregarded—between 2008 and 2014, leading EU nations gradually cut their military spending. The 2008 war in Georgia failed to serve as a wake-up call for European countries. Instead, it set a precedent of impunity for Russia and paved the way for future aggression.

The US and the Reset Policy

At the 2009 Munich Security Conference, U.S. Vice President Joe Biden announced the "reset" policy between the two countries. A key reason for this policy was the U.S. shifting its strategic focus toward Asia, primarily because of the China factor. President Obama aimed to increase U.S. influence in the Asia-Pacific region, which required stable relations with Russia.

In March 2014, Moscow illegally annexed Crimea and supported separatist movements in the Donbas. However, the West responded with insufficient sanctions. The Obama administration wanted to avoid escalation with Russia, so the U.S. only supplied non-lethal military aid to Ukraine. v

Obama's passive approach toward Ukraine continued until the end of his term. Although the U.S. provided Ukraine with military equipment, it was strictly non-lethal (such as night vision gear, body armor, and medical supplies). Obama explained this decision by stating: "Our goal is not to equip Ukraine with lethal weapons against Russia, because frankly, the Ukrainian army will never defeat Russia. Instead, our goal is to find a diplomatic solution".

On March 26, 2014, Obama stated that neither Georgia nor Ukraine were on the path to joining NATO. For Russia,vithis statement was another concession and a clear signal that Moscow's aggressive policy was working.vii

Keeping its ally Bashar al-Assad in power in Syria gave the Kremlin a chance to gain geopolitical advantages. On August 20, 2012, Barack Obama declared that the use of chemical weapons was a "red line" for the United States. Despite this, when Assad actually used chemical weapons, the U.S. did not take any effective action in response.

The 2022 Ukraine War as a Consequence

On February 24, 2022, Russia launched a full-scale war in Ukraine. Years of soft, appeasement policies toward Moscow played a major role in leading up to this event.viiiix

In 2021, just months before the war began, trade turnover between Russia and the EU reached a record 247 billion euros, which helped Moscow build a 600 billion dollar reserve. Beyond this financial boost, despite an existing embargo, Russia purchased 346 million euros worth of military equipment from 10 EU member states between 2015 and 2020.

At the same time, the U.S. "reset" policy, the refusal to supply Ukraine with lethal weapons after the annexation of Crimea, and the ignored red lines in Syria severely undermined America's deterrence status in the eyes of the Kremlin. On February 24, 2022, Russia launched its so-called "special military operation," which became the largest military conflict on European soil since World War II.

Recommendations

The historical record examined in this paper suggests that a more effective Western approach after 2008 would not necessarily have required direct military confrontation with Russia. Rather, deterrence could have been strengthened through measures designed to reduce Moscow's economic leverage, constrain its military modernization, and increase the costs of further aggression.

1. Energy Diversification

Following Russia's 2008 aggression against Georgia, the EU and the United States should have accelerated efforts to diversify European energy supplies and reduce dependence on Russian hydrocarbons. Such a policy would have constrained one of Moscow's most important sources of economic and political leverage while reducing the resources available to support Russia's military modernization and future external aggression.

Instead, European states continued to deepen their energy relationship with Russia. Germany provides a particularly important example: its decision to phase out nuclear power, a process completed in 2023, increased the importance of alternative energy sources, including Russian gas, during the subsequent period. Greater diversification after 2008 could therefore have reduced both Europe's strategic vulnerability and Russia's ability to use energy interdependence as an instrument of influence.

2. Military and Technological Restrictions

A second priority should have been the systematic restriction of Western military and dual-use technology transfers to Russia. The Kremlin's military modernization depended in part on access to Western technologies, equipment, and expertise. A comprehensive military and technological embargo following the 2008 war could therefore have imposed meaningful constraints on Russia's future military capabilities.

Rather than continuing military cooperation through mechanisms such as the NATO-Russia Council and joint exercises, Western governments could have progressively

suspended such cooperation while restricting the transfer of military and strategically relevant technologies. Following the annexation of Crimea in 2014, sanctions and export restrictions were introduced, but their implementation was not comprehensive. Earlier and more consistent restrictions could have increased the costs of Russian military modernization before the full-scale invasion of Ukraine.

3. Sustained Defense Investment and Deterrence

Finally, Western states should have maintained or increased defense spending after 2008 rather than allowing prolonged reductions in military capabilities. Credible deterrence depends not only on political statements but also on the demonstrable capacity and willingness to respond to aggression.

A sustained increase in defense investment would have strengthened NATO's conventional deterrence, particularly on its eastern flank, while improving readiness, resilience, and the Alliance's ability to respond to a rapidly deteriorating security environment. The 2008 war should therefore have been treated not as a peripheral regional crisis but as an early warning that European security required renewed investment in collective defense.

CONCLUSION

The trajectory examined in this paper demonstrates that Russia's increasing assertiveness was enabled not only by the Kremlin's revisionist ambitions but also by a Western policy that repeatedly prioritized engagement, economic interdependence, and avoidance of escalation over credible deterrence. The 2008 Russia-Georgia war, the annexation of Crimea, and Russia's intervention in Syria provided successive warnings about Moscow's willingness to challenge the existing international order, yet Western responses remained limited and largely reactive. Continued economic ties, energy dependence, insufficient military investment, and inconsistent political and technological restrictions reduced the costs associated with Russian aggression and created greater space for further escalation. While it cannot be established that a different Western policy would have prevented the 2022 invasion of Ukraine, earlier energy diversification, stronger defense capabilities, and comprehensive restrictions on military and strategic technologies could have increased the costs of Russian aggression and strengthened deterrence. The central lesson is clear: diplomacy remains necessary, but without credible economic, military, and political consequences, engagement can unintentionally enable further revisionist behavior.

Photo: Kremlin

[i] Tom Parfitt, "Anna Politkovskaya: The Only Good Journalist," *The Guardian*, October 10, 2006, https://www.theguardian.com/world/2006/oct/10/russia.media.
[ii] J. Berger, "Analyzing Vladimir Putin's Rhetoric and Its Implications for Russian Grand Strategy" (Master's thesis, School of Advanced Air and Space Studies, 2016), Homeland Security Digital Library, https://www.hsdl.org/c/view?docid=812653.
[iii] Eurostat, "Energy Production and Imports," European Commission, 2014, https://ec.europa.eu/eurostat/statistics-explained/index.php/Energy_production_and_imports.
[iv] Stockholm International Peace Research Institute, "SIPRI Military Expenditure Database," 2024, https://www.sipri.org/databases/milex.
[v] The White House, Office of the Press Secretary, "Remarks by President Obama and Chancellor Merkel in Joint Press Conference," February 9, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/02/09/remarks-president-obama-and-chancellor-merkel-joint-press-conference.
[vi] Charap, Treyger, and Geist, *Understanding Russia's Intervention in Syria*.
[vii] Barack Obama, "Remarks by the President to the White House Press Corps," August 20, 2012, The White House, Office of the Press Secretary, https://obamawhitehouse.archives.gov/the-press-office/2012/08/20/remarks-president-white-house-press-corps.
[viii] Eurostat, "Energy Represented 62% of EU Imports from Russia."
[ix] Investigate Europe, "EU Member States Exported Weapons to Russia After the 2014 Embargo," March 16, 2022, https://www.investigate-europe.eu/posts/eu-states-exported-weapons-to-russia.

Strategic Security Initiative (SSI)

ADVANCING INSIGHT ON GLOBAL SECURITY

SSI Youth Voices