FREE NETWORK
POLICY BRIEF SERIES #AcademicsStandWithUkraine

Anna Anisimova, SITE,
Ksenia Rundin, CSSC at SSE
March 2026

Antagonistic Information Threats: Lessons from Ukraine

Russia's full-scale invasion of Ukraine highlights how modern conflict increasingly relies on antagonistic information threats alongside military force. This policy brief examines how such threats operate and what lessons they offer for European resilience. First, it outlines a framework through which hostile actors gradually weaken societies' capacity to interpret events and trust institutions. Second, the brief analyzes Ukrainian cyber operations, highlighting that sustained defensive investment can reduce destructive impact even as attack activity intensifies. The brief further examines the economic implications, showing that antagonistic threats create continuous fiscal pressure as monitoring, detection, and incident response become permanent public expenditures rather than temporary crisis measures. Finally, the brief draws policy implications for Europe, stressing the need to treat cyber and information resilience as macro-critical infrastructure and to strengthen coordination across policy domains.

Introduction

Ukraine's experience since the full-scale invasion of 2022 illustrates how antagonistic threats operate in contemporary conflict. The war demonstrates that modern confrontation extends far beyond conventional military force. Instead, it functions as a hybrid system in which military, informational, economic, and political instruments are combined into a coordinated architecture of pressure. While this dynamic is most visible in active war, its underlying mechanisms are not confined to the battlefield. Similar forms of antagonistic pressure are increasingly directed at European societies despite the absence of open military confrontation.

Within this broader system, information threats have become particularly significant, largely due to technological change and the digitalization of communication. Networked information environments allow hostile actors to combine cyber operations, disinformation campaigns, and other forms of manipulation at low cost and large scale, amplifying the effects of other forms of pressure. Information operations can shape how events are interpreted, undermine institutional trust, and influence political behavior, often reinforcing technical disruption or economic coercion.

This brief focuses on antagonistic information threats — hostile activities that include disinformation campaigns, cyber operations, and other forms of manipulation targeting the information environment. We first outline a structural framework for understanding the targets and effects of such threats. We then examine how cyber operations have been used in Ukraine and assess their associated costs. The brief concludes with policy lessons relevant for strengthening resilience in European societies.

Layers of Antagonistic Information Influence

Understanding antagonistic information threats requires moving beyond viewing disinformation or cyber incidents as isolated events. Instead, these activities form a structured and multi-layered architecture of pressure aimed at gradually degrading democratic governance. Rather than aiming for immediate institutional breakdown, these operations gradually weaken a society's capacity to interpret events, trust institutions, and act collectively across four interconnected layers: cognitive, institutional, informational, and behavioral. This four-layer framing synthesizes Ukraine's wartime practice with established research on cognitive warfare and decision-making manipulation, hybrid warfare, and institutional effectiveness (NATO STO, n.d.; Havlík & Horáček, 2026; Tsybulska, 2023; World Bank, 2017).

At the cognitive layer, hostile actors target how individuals interpret reality, shaping threat perception, responsibility attribution, and identity boundaries. This dynamic is well documented in research on cognitive warfare and reflexive control, which demonstrates that perception manipulation can redirect strategic decision-making without direct confrontation (Havlík & Horáček, 2026; Thomas, 2004). By exploiting uncertainty, fear, and emotional triggers, adversaries influence how citizens understand crises before institutional responses even occur. Cognitive distortion thus lays the foundation for broader destabilization.

At the institutional layer, hostile actors target trust in government, elections, and public authority. Evidence from hybrid warfare analysis demonstrates that weakening institutional legitimacy degrades both crisis response and democratic resilience (OECD, 2022; World Bank, 2017). As Tsybulska (2023) argues, delegitimization, rather than outright destruction, is often the central objective of a hybrid strategy. When public trust erodes, policy implementation fragments, and crisis communication loses authority.

The informational layer addresses narrative dominance and agenda-setting. Hostile actors use saturation, repetition, and cross-platform amplification to ensure that adversarial frames define the terms of public debate (McCombs & Shaw, 1972; Paul & Matthews, 2016). The goal is not simply to spread falsehoods but to normalize certain interpretations over time, embedding them into how societies process political reality (Tsybulska, 2024).

Finally, the behavioral layer translates perception and narrative control into observable outcomes, from voting behavior and protest mobilization to compliance with policy measures and support for defense decisions. Research on misinformation and political behavior demonstrates that even marginal shifts in turnout, polarization, or policy support can generate significant strategic consequences (Allcott & Gentzkow, 2017). Behavioral influence does not require majority conversion; small distortions at scale can reshape political outcomes.

Ukraine's post-2022 experience shows that antagonistic information threats function as a long-term governance pressure system, designed for erosion. This is why recognizing the layered architecture of these threats is essential for building durable resilience.

Threats at the Operational Level: Lessons from Ukraine

Ukraine's wartime experience illustrates how antagonistic information threats operate in practice, particularly through cyber operations. Unlike kinetic warfare, cyber operations continue even during ceasefires: they are relatively low-cost, scalable, and persistent, generating both technical disruption and information that can later be exploited in influence campaigns.

The Computer Emergency Response Team of Ukraine (CERT-UA) recorded 4,315 cyber incidents in 2024, nearly a 70% increase over 2023 and more than triple the 2021 level (SSSCIP/CERT-UA, 2025c). In the first half of 2025 alone, incidents increased by a further 17% (SSSCIP/CERT-UA, 2025b). These figures reflect strategic structural pressure, as shown in Table 1.

Table 1. Registered cyber incidents in Ukraine, 2021–2024

Year	Total incidents	Critical & high-severity incidents
2021	1,350	403
2022	2,194	1,048
2023	2,543	367
2024	4,315	59

Source: CERT-UA / State Service of Special Communications and Information Protection of Ukraine (SSSCIP), Russian Cyber Operations: Analytics for the Second Half of 2024.

At the same time, a parallel trend deserves attention: while overall incident volume rose sharply, critical and high-severity incidents

declined by 94% between 2022 and 2024 (SSSCIP/CERT-UA, 2025a). Ukrainian authorities attribute this to strengthened monitoring networks, early detection mechanisms, and international cooperation. The policy conclusion is clear: sustained defensive investment reduces destructive impact even as attack frequency increases.

The operational model has also evolved. Rather than prioritizing spectacular disruption, campaigns increasingly emphasize persistent access, credential theft, and selective data exfiltration, so-called 'steal and go' tactics (SSSCIP/CERT-UA, 2025b). The objective is chronic degradation rather than dramatic collapse. Data theft supports later narrative exploitation; minor disruption normalizes instability; repeated low-grade incidents strain administrative capacity.

This shift aligns with the broader strategic goal identified in Ukrainian cybersecurity reporting: producing distrust, paralysis, delayed response, societal fatigue, and long-term strategic advantage. The sectoral and methodological breakdown confirms this pattern (Table 2).

Artificial intelligence (AI) further accelerates this dynamic. Large-scale content saturation campaigns, such as the Pravda/Portal Kombat network, have been documented flooding digital ecosystems and targeting AI retrieval environments (American Sunlight Project, 2025; Sadeghi & Blachez, 2025). While academic debate continues over the scale of LLM manipulation (Alyukov et al., 2025), the strategic investment in content flooding is well documented.

Generative AI reduces the marginal cost of producing multilingual disinformation. CERT-UA has also identified indications of AI-assisted scripting in phishing and malware deployment (SSSCIP/CERT-UA, 2025b). As Havlík and Horáček (2026) warn, AI increasingly enables the precision targeting of cognitive vulnerabilities, thereby compressing defenders' response time.

Table 2. Target sectors and attack methods in Ukraine in 2024

Target sector/ Method	Jan–Jun 2024	Jul–Dec 2024	Change
Target:			
Government	473	665	+41%
Local authorities	542	831	+53%
Military	276	502	+82%
Energy	124	127	+2%
Telecom & IT	26	37	+42%
Method:			
Malware distribution	531	1,123	+112%
Malware infection	196	320	+63%
Severity:			
Critical & high	48	11	−77%

Source: CERT-UA/SSSCIP, Russian Cyber Operations: Analytics for the Second Half of 2024. Sector figures are incident counts; method figures reflect malware-specific incidents.

These dynamics illustrate how cyber operations generate effects across the four layers of antagonistic information influence identified earlier. Repeated incidents and data leaks shape the informational environment; narrative exploitation of stolen or manipulated data affects how events are cognitively interpreted; persistent disruptions undermine institutional credibility and crisis response; and accumulated uncertainty ultimately influences political and societal behavior.

Crucially, antagonistic information threats do not operate alone. They are part of a synchronized

system of persistent pressure. Cyber operations, Foreign Information Manipulation and Interference, economic coercion, electronic warfare, and kinetic activity are integrated into a unified strategy. Ukrainian authorities report temporal synchronization between cyber intrusions, energy-sector targeting, and missile strikes (SSSCIP/CERT-UA, 2025a). Narrative campaigns frame events before and after disruption; cyber operations generate exploitable material; economic pressure increases uncertainty; kinetic or electronic actions amplify fear. The compound effect exceeds what any single domain could achieve on its own.

Ukrainian experience highlights vulnerabilities relevant for Europe more broadly. Hybrid pressure operates as a synchronized, multi-domain system in which military, informational, economic, and political instruments reinforce one another. European governance, however, addresses these domains through separate institutional channels. Energy security, cyber defence, strategic communications, and democratic resilience are managed in distinct policy silos with different authorities and threat perceptions. This fragmentation creates exploitable gaps: an adversary operating through tightly coordinated cross-domain pressure can exploit exactly the delays and blind spots that institutional separation produces.

The lesson from Ukraine is therefore not limited to wartime resilience. Even without open conflict, antagonistic actors can pursue gradual systemic pressure by targeting infrastructure, information, economic vulnerabilities, and institutional trust simultaneously. Effective resilience, therefore, requires moving beyond sectoral responses toward integrated governance capable of anticipating and responding to coordinated cross-domain pressure.

Economic Costs of Antagonistic Information Threats

Antagonistic information threats are persistent and structurally embedded, which means their economic implications extend beyond isolated incidents. Ukraine's experience provides a rare empirical case showing how these costs accumulate and how sustained investment can mitigate them. Hybrid pressure does not produce only one-off destruction; it generates continuous fiscal demand. Monitoring, detection, and incident response systems have therefore become permanent budget items rather than crisis expenditures.

In 2024 alone, national monitoring systems processed hundreds of billions of telemetry events, identified around 3 million security events, and confirmed 1,042 cyber incidents requiring formal response (SSSCIP, 2024). These figures illustrate that antagonistic threats impose a constant administrative and financial burden, underscoring the fiscal consequences of inaction.

Ukraine's cybersecurity market reached approximately 138 million USD in 2024, having quadrupled over eight years (SSSCIP, 2024). This growth reflects systemic adaptation under sustained pressure rather than discretionary digital modernization. The statistics in Table 1 show that investment did not eliminate the threat, but it fundamentally reduced its destructive impact. The burden falls disproportionately on public

administration. With 76% of recorded incidents targeting government, local authorities, and the defense-industrial sector, the fiscal weight of cybersecurity concentrates where the budgets are most constrained. In this way, the institutions most essential to democratic governance bear the highest cost of defence.

Beyond direct-response spending, antagonistic threats impose systemic economic costs. Insurance premiums rise while cyber coverage narrows; compliance costs increase under frameworks such as NIS2, and procurement and crisis coordination become slower and more complex. As public administration becomes a primary target, trust and institutional credibility weaken, raising coordination costs across markets and public systems. As a result, governance efficiency itself becomes economically vulnerable.

At the same time, the costs of inaction are substantial. At the European level, ENISA estimates total cyber-related losses over five years at approximately €300 billion, with Germany alone reporting €205.9 billion in losses in 2023 (Nagy, 2023). While these figures do not isolate state-linked hybrid operations, they indicate the fiscal environment in which antagonistic threats operate and suggest a scale of what unmitigated exposure would cost.

The EU's persistent security workforce deficit of 260,000 to 500,000 specialists (ENISA, 2024) further constrains the capacity for the type of sustained defensive investment that Ukraine's experience shows to be effective.

Table 3 highlights a central policy lesson. In Ukraine, both the number of detected threats and the capacity to identify them increased sharply, while the share of destructive incidents declined significantly. This demonstrates that rising incident volume does not necessarily translate into rising damage. It thus indicates that the economic trade-off is not between security spending and fiscal savings, but between investing in preventive resilience and absorbing escalating systemic costs.

Table 3. The Returns on Sustained Investment, Ukraine

Indicator	Baseline	Post-investment outcome
Cyber incident detected	1,350 (2021)	4,315 (2024), reflects expanded detection capacity
Critical/high-severity incidents	1,048 (2022)	59 (2024), a 94 % reduction
Cybersecurity market size	~USD 34m (2016)	~USD 138m (2024)

Sources: CERT-UA/SSSCIP (2025a, 2025b, 2025c); SSSCIP (2024); ENISA (2024); Howden (2025).

In economic terms, resilience reduces the probability of high-impact shocks, whereas delayed investment merely defers their costs. For European policymakers, cyber and information resilience must be treated as macro-critical infrastructure, with financial consequences extending well beyond IT systems into fiscal stability, labour markets, and long-term growth.

Conclusions

Ukraine's experience since 2022 demonstrates that antagonistic information threats must be treated as a systemic governance challenge, not just a communication problem. Operating simultaneously across cognitive, institutional, informational, and behavioral layers, these threats aim to erode decision-making capacity rather than

trigger immediate collapse. The strategic objective is gradual fragmentation of perception, trust, narrative coherence, and ultimately political action. For policymakers, the implication is straightforward: resilience must be built across all four layers.

Moreover, Ukraine's operational data demonstrates that antagonistic information threats are persistent, adaptive, AI-accelerated, and strategically synchronized. Resilience must therefore be systemic, coordinated, and anticipatory, not reactive and sector-bound.

Ukrainian experience shows that sustained investment did not eliminate cyber pressure, but it dramatically reduced high-severity impact while expanding detection capacity. At the same time, the burden of defense falls disproportionately on public administration. Treating resilience spending as macro-critical infrastructure investment could be part of the solution.

References

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives, 31*(2), 211–236.

Alyukov, M., Makhortykh, M., Voronovici, A., & Sydorova, M. (2025). LLMs grooming or data voids? *Harvard Kennedy School Misinformation Review, 6*(5).

American Sunlight Project. (2025, February 26). Russian propaganda may be flooding AI models: The Pravda network and risks to AI information integrity.

European Union Agency for Cybersecurity (ENISA). (2024). 2024 report on the state of cybersecurity in the Union.

Havlík, M., & Horáček, J. (2026). War is a mind game: Countering weaponized information. NATO Defense College.

Howden (2025). Rebooting growth. Howden's 2025 cyber insurance report.

McCombs, M., & Shaw, D. (1972). The agenda-setting function of mass media. *Public Opinion Quarterly, 36*(2), 176–187.

Nagy, C. (2023, December 11). 2024 cybersecurity predictions and emerging threats in Germany. SecurityBridge.

NATO Science and Technology Organization (NATO STO). (n.d.). Cognitive warfare: NATO chief scientist research report.

OECD. (2022). Building Trust to Reinforce Democracy: Main Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions, Building Trust in Public Institutions. OECD Publishing.

Paul, C., & Matthews, M. (2016). The Russian "firehose of falsehood" propaganda model. *RAND Corporation*.

Sadeghi, M., & Blachez, I. (2025, March 6). A well-funded Moscow-based global 'news' network has infected Western artificial intelligence tools worldwide with Russian propaganda. NewsGuard.

State Service of Special Communications and Information Protection of Ukraine (SSSCIP) / CERT-UA. (2025a). Russian Cyber Operations: Analytics for H2 2024.

State Service of Special Communications and Information Protection of Ukraine (SSSCIP) / CERT-UA. (2025b). Russian Cyber Operations: Analytics for H1 2025.

State Service of Special Communications and Information Protection of Ukraine (SSSCIP) / CERT-UA. (2025c). CERT-UA recorded 4,315 cyber incidents in 2024.

Thomas, T. (2004). Russia's reflexive control theory and the military. *Journal of Slavic Military Studies, 17*(2), 237–256.

Tsybulska, L. (2023). Hybrid warfare in Ukraine. Carnegie Council for Ethics in International Affairs.

Tsybulska, L. (2024). Russian culture is a shining Trojan horse with tanks, bombs, and missiles inside. Detector Media.

World Bank. (2017). World development report 2017: Governance and the law.

Anna Anisimova

Stockholm Institute of Transition Economics
anna.anisimova@hhs.se
https://www.hhs.se/sv/persons/a/anisimova-hanna/

Anna Anisimova obtained her PhD in Economics from Donetsk National University in 2010, with her doctoral thesis focused on Industrial Management. She then worked there as an Assistant Professor at the Department of Business Statistics and Economic Cybernetics. In June 2020, she joined SITE and currently holds the position of Researcher. Her main research interests are in gender economics, human capital development, and transition economics.

Ksenia Rundin

CSSC at SSE
ksenia.rundin@hhs.se
https://www.hhs.se/en/persons/r/rundin-ksenia-mischa/

Ksenia Rundin obtained a PhD in Business Administration from the Stockholm School of Economics in 2024 and currently holds a position as a postdoctoral fellow at the Center for Statecraft and Strategic Communication at the Stockholm School of Economics. Her research examines contemporary propaganda and disinformation, with a particular focus on how strategies developed during the Cold War have evolved in the digital age through social media and emerging cyber threats.

freepolicybriefs.com

The Forum for Research on Eastern Europe and Emerging Economies is a network of academic experts on economic issues in Eastern Europe and the former Soviet Union at BEROC (Vilnius), BICEPS (Riga), CenEA (Szczecin), ISET-PI (Tbilisi), KSE (Kyiv) and SITE (Stockholm). The weekly FREE Network Policy Brief Series provides research-based analyses of economic policy issues relevant to Eastern Europe and emerging markets. Opinions expressed in policy briefs and other publications are those of the authors; they do not necessarily reflect those of the FREE Network and its research institutes.

FREE NETWORK