



POLICY PAPER

BEYOND DEFENCE

A PROACTIVE STRATEGY FOR THE WEST IN THE INFORMATION DOMAIN

| PEKKA KALLIONIEMI |

NOVEMBER 2025

RKK
ICDS

RAHVUSVAHELINE KAITSEURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI • ESTONIA

Title: Beyond Defence: A Proactive Strategy for the West in the Information Domain
Author: Kallioniemi, Pekka
Publication date: November 2025
Category: Policy Paper

Cover page photo: An anti-vaccine rally in front of the Lincoln Memorial in Washington on 23 January 2022. AP Photo/Patrick Semansky/Scanpix.

Keywords: authoritarian regime, countermeasures, democracy, disinformation, influence campaigns, information operations, propaganda, China, European Union, NATO, United States, Russia

Disclaimer: The views and opinions contained in this analysis are those of its authors only and do not necessarily represent the positions of the International Centre for Defence and Security or any other organisation.

ISSN 2228-2068

© International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

CONTENTS

List of Abbreviations	III
About the Author	III
Introduction	1
1. Strategic Threat Landscape	1
1.1. Structural Advantages of Authoritarian States	2
1.2. Disinformation Tactics	3
1.3. Asymmetry in the Information War	5
2. Uneven Battleground: Disparities in Disinformation Funding	6
2.1. Authoritarian Investment in Propaganda	7
2.2. Collaborative Narrative Ecosystems	7
2.3. EU's Counter-Disinformation Funding	8
2.4. Structural Constraints in Liberal Democracies	8
3. The US Variable: A Strategic Uncertainty	8
Conclusion and Recommendations	10

LIST OF ABBREVIATIONS

AfD	Alternative for Germany (<i>Alternative für Deutschland</i>)
EDMO	European Digital Media Observatory (EU)
EEAS	European External Action Service (EU)
EMIF	European Media and Information Fund (EU)
FBK	Anti-Corruption Foundation (<i>Фонд борьбы с коррупцией</i> , Russia)
FERMI	Fake News Risk Mitigator (EU)
FIMI	foreign information manipulation and interference
GEC	Global Engagement Center (US)
IRA	Internet Research Agency (Russia)
MAGA	Make America Great Again
MFF	Multiannual Financial Framework
OSINT	open-source intelligence
PLA	People's Liberation Army (China)
StratCom COE	Strategic Communications Centre of Excellence (NATO)
VIGILANT	Vital Intelligence to Investigate Illegal Disinformation (EU)

ABOUT THE AUTHOR

PEKKA KALLIONIEMI

Dr Pekka Kallioniemi is an expert on social media and disinformation, who has worked as an independent consultant and a postdoctoral researcher on human-technology interaction at Tampere University (Finland). In addition to his academic interest in state-of-the-art technologies, he has also studied Russian online information operations and disinformation. In his current research, he combines these topics, focusing on how online information operations and disinformation may change in the future with the adoption of technologies such as ChatGPT, deep fakes, and generative AI. Dr Kallioniemi has published the popular *Vatnik Soup* series since October 2022 and has regularly commented to national and inter-national media on these issues. Since January 2023, he has also been a columnist for the Brit-ish newspaper *Byline Times*. Dr Kallioniemi's work has been covered in *The Wall Street Journal*, *The Washington Post*, *The New York Times*, and *Die Welt*.

INTRODUCTION

The liberal democratic world is losing the information war. For over a decade, authoritarian states – led by Russia and China – have developed and deployed sophisticated influence campaigns designed to erode public trust, polarise societies, and undermine the legitimacy of democratic institutions. These campaigns are not isolated disruptions; they are part of a broader, long-term strategy to reshape the global order in their favour by weakening the democratic west from within.

While liberal democracies have built strong norms around transparency, press freedom, and pluralism, these same strengths have been exploited by authoritarian regimes as vulnerabilities. The openness of western societies allows adversaries to amplify disinformation at scale, often faster than it can be countered. Meanwhile, the closed and censored information environments of Russia and China make it nearly impossible to inject counter-narratives into their populations. This structural asymmetry is central to the ongoing contest.

Current investments in information resilience pale in comparison to the scale of the threat

The threat is compounded by significant disparities in funding, speed of decision-making, and institutional agility. Authoritarian regimes can rapidly deploy resources, align messaging across state and non-state actors, and reallocate budgets without public scrutiny. In contrast, democratic responses remain fragmented, reactive, and chronically

underfunded. NATO, the EU, and national governments have made important strides, but current investments in information resilience pale in comparison to the scale of the threat.

The result is a dangerous imbalance. Russia’s ‘firehose of falsehood’ model floods the global information space with confusion and cynicism. China combines infrastructure investments with soft power strategies and narrative control. Both states actively support pro-authoritarian or anti-EU actors in the west, exploiting political divides and seeding mistrust. These efforts are amplified by social media superspreaders, algorithmic incentives, and the erosion of public trust in traditional institutions.

To shift this trajectory, the west must stop playing defence. It must reclaim the initiative by understanding the adversary’s advantages, disrupting their tactics, and investing in its own narrative power. This paper outlines the current threat landscape and proposes a set of proactive, scalable strategies for NATO, the EU, and national governments to respond – before the asymmetry becomes irreversible.

Authoritarian regimes – particularly Russia and China – have built coordinated, well-funded, and ideologically coherent systems for conducting influence operations

1. STRATEGIC THREAT LANDSCAPE

The modern information war is fundamentally asymmetrical. Authoritarian regimes – particularly Russia and China – have built coordinated, well-funded, and ideologically coherent systems for conducting influence operations both at home and abroad. Liberal democracies, by contrast, remain fragmented, under-resourced, and institutionally constrained. This section outlines the key structural advantages, tactical models, and resource disparities that define the current threat landscape.

1.1. STRUCTURAL ADVANTAGES OF AUTHORITARIAN STATES

Authoritarian regimes possess built-in advantages that make them highly effective actors in the information domain. These advantages are both institutional and historical, enabling autocracies to execute large-scale influence operations with speed, discipline, and impunity.

Strategic decisions within these systems are made quickly and centrally, without the need for legislative approval, interagency coordination, or public scrutiny. Messaging campaigns can be launched, adapted, or withdrawn at a moment's notice, without legal or political constraints. There is no obligation to consult with diverse stakeholders, respond to media criticism, or justify actions to the public. This allows authoritarian regimes to act with a degree of agility and coherence that liberal democracies, by design, do not possess.

In addition, autocracies tightly control their domestic information spaces. Independent media are suppressed, dissenting voices are silenced, and state narratives are disseminated without competition. This monopoly on internal communication allows for the full-spectrum projection of external disinformation, unencumbered by internal contradiction or resistance.

In the case of Russia, these structural advantages are compounded by a longstanding tradition of psychological operations and behavioural influence. Dating back to the Soviet era – and in many ways continuing practices developed by the KGB – Russian statecraft has emphasised the strategic manipulation of perception, the exploitation of cognitive biases, and the disruption of adversarial societies through disinformation. This tradition informs the design and execution of sophisticated, high-volume influence campaigns, often deployed across western social media platforms with the aim of destabilisation rather than persuasion.

Authoritarian regimes also benefit from resource flexibility. They can reallocate funding from social sectors, such as healthcare or education, toward information operations and foreign influence efforts with minimal

political cost. Unlike democracies, where such reallocation would spark public backlash, political opposition, and media scrutiny, autocracies face little to no resistance in prioritising propaganda over public welfare. This enables sustained investment in information warfare, even at the expense of domestic well-being.

These conditions provide authoritarian states with a decisive edge in the global information environment. They can act faster, speak louder, and operate in a more strategically unified manner than their democratic counterparts – all while shielding their operations from internal dissent or external transparency.

To summarise, authoritarian regimes possess systemic strengths that enhance their capacity for information warfare:

- **Centralised decision-making:** Strategic messaging decisions can be made rapidly without legislative scrutiny, public transparency, or media oversight. Campaigns can be launched or altered in real time, with full institutional alignment.
- **Controlled information ecosystems:** Regimes like Russia and China maintain near-total control over their domestic information spaces. Independent journalism is suppressed, while state media and algorithmic censorship ensure narrative dominance.
- **Psychological operations legacy:** Russia, in particular, draws from a Soviet-era tradition of psychological operations and behavioural influence. This informs the design of contemporary disinformation efforts.
- **Flexible resource allocation:** Authoritarian states can divert funds from social sectors to information warfare without public resistance. Budgetary opacity allows for the covert financing of propaganda networks.

1.2. DISINFORMATION TACTICS

1.2.1. THE FIREHOSE OF FALSEHOOD

One of the most disruptive tactics in Russia's modern propaganda arsenal is the 'firehose of falsehood' model, a term coined by RAND researchers to describe a disinformation strategy that is high in volume, multichannel, fast, repetitive, and unconcerned with truth or consistency.¹ Rather than persuading through evidence or logic, this method seeks to overwhelm audiences, confuse public discourse, and erode trust in objective reality.

The Internet Research Agency (IRA), directed by Yevgeny Prigozhin until his death in 2023, operationalised this model on an industrial scale. Hundreds of operatives working in shifts generated a relentless stream of pro-Kremlin messaging across social media platforms, comment sections, and fringe websites. These campaigns targeted a wide array of audiences with emotionally charged but often contradictory narratives – for example, depicting Ukraine as both a helpless vassal of the west and an existential threat to Russian security.²

Russian propaganda systematically attempts to shift attention away from the country's own internal dysfunction

A core element of this approach is narrative deflection. Russian propaganda systematically attempts to shift attention away from the country's own internal dysfunction by highlighting or fabricating flaws in western societies. Stories of US political polarisation, European 'wokeness', immigration crises, or declining birthrates are promoted to imply

that liberal democracies are in terminal decline.³

This tactic helps obscure a stark reality: Russia itself is plagued by deep structural problems, including a shrinking and ageing population, low life expectancy, widespread substance abuse, one of the world's highest divorce rates, and a stagnant economy reliant on fossil fuel exports.⁴ Rather than address these issues, the Kremlin builds external narratives to divert domestic frustrations and international criticism.

One of the most powerful propaganda narratives constructed through the firehose model is the image of 'traditional, conservative Russia' standing as a bulwark against a 'decadent and decaying west'. Despite internal crises, the Kremlin has successfully exported this myth to international audiences – particularly among conservative movements in Europe, North America, and the global south. Russian state media, pseudo-academic influencers, and covert financial operations have all been used to position Russia as a defender of 'Christian civilisation', 'family values', and 'sovereignty' against western liberalism.⁵

This narrative is strategically deployed to support pro-Kremlin political figures and movements in democratic societies. In the United States, Russian disinformation campaigns have amplified Donald Trump and the Make America Great Again (MAGA) movement, often targeting elections, vaccines, immigration, and NATO.⁶ In Germany, the far-right AfD has received direct amplification from Russian media and state-linked trolls, particularly in the context

¹ Christopher Paul, Miriam Matthews, "The Russian 'Firehose of Falsehood' Propaganda Model Why It Might Work and Options to Counter It," *Rand Corporation*, 2(7) (July 2016): 1–10.

² Savvas Zannettou, Tristan Caulfield, William Setzer, Michael Sirivianos, "Who Let the Trolls Out? Understanding State-Sponsored Trolls," *Proceedings of the 10th ACM Web Science Conference* (June 2019): 353–362; US Department of Justice, "DOJ Disrupts Russian Influence Operation Targeting U.S. Audiences," DOJ, 4 September 2024;

³ Kathleen Hall Jamieson, "How Russian hackers and trolls exploited US media in 2016," *Proceedings of the American Philosophical Society*, 163(2) (March 2020): 122–135; Center for Countering Disinformation (Ukraine), "Where the Kremlin Gets Money to Boost Propaganda Funding," CPD, 7 October 2024.

⁴ Oleksii Artemchuk, "Russia to Increase State Propaganda Spending," *Ukrainska Pravda*, 7 October 2024; "How Much Does Russia Spend on Propaganda?," *Filter Ukraine*, 2024.

⁵ Steve Tatham, *Information Operations: Facts, Fakes, Conspiracies* (Howgate Publishing, 2024); Michael Scholtens, Pedro Pizano, Max Karpawich, and Guthrie Kuckes, *The Disinformation Economy* (The Carter Center, McCain Institute, 2024).

⁶ Jamieson, "How Russian hackers"; DOJ, "DOJ Disrupts Russian Influence."

of anti-aid to Ukraine and anti-EU sentiment.⁷ In Romania, figures like Călin Georgescu and George Simion have echoed Kremlin narratives around ‘national sovereignty’, anti-globalism, and western corruption.⁸

Elsewhere, Hungarian Prime Minister Viktor Orbán has maintained close ties with Moscow, regularly opposing EU sanctions and echoing Kremlin messaging around ‘illiberal democracy’. In France, Marine Le Pen’s party received loans from Russian banks and favourable coverage from state-aligned outlets, supporting her anti-EU and anti-NATO stance.⁹

The firehose of falsehood is not merely a tool of deception – it is a mechanism for identity construction and influence projection

In essence, the firehose of falsehood is not merely a tool of deception – it is a mechanism for identity construction and influence projection. It allows Russia to define itself to foreign audiences not by what it is, but by what it opposes. The success of this narrative, despite glaring contradictions between the image and Russia’s internal realities, demonstrates the power of coordinated, unapologetic disinformation to reshape global perceptions and co-opt segments of democratic societies for geopolitical ends.

1.2.2. INFORMATION LAUNDERING

One of the more sophisticated tactics employed in Russian disinformation campaigns is information laundering – a process by which false or misleading narratives are gradually cleansed of their origin and infused with the appearance of legitimacy. This tactic mirrors the logic of financial money laundering: just as illicit funds are funnelled through layers of transactions to appear clean, disinformation is passed

through various channels – blogs, social media accounts, fringe outlets, and sympathetic commentators – until it emerges in more credible-seeming forums.

In practice, a fabricated or heavily distorted claim might first appear on a dubious blog or in a fringe outlet with a known pro-Kremlin slant. From there, it is picked up and amplified by social media influencers, ‘alternative media’ platforms, or anonymous accounts that present the narrative as independent analysis. Through repetition and cross-referencing via loosely affiliated actors, the original falsehood becomes detached from its propagandistic origins. Eventually, the narrative may surface in more mainstream debate, cited by populist politicians or echoed by seemingly neutral commentators – giving it a veneer of authenticity.

This method not only helps spread disinformation more widely but also creates plausible deniability for state actors. By outsourcing the message to intermediaries – especially those in the west – Kremlin-linked narratives can circulate without direct attribution, complicating efforts to trace and debunk their origins. The process blurs the line between grassroots discourse and state-sponsored manipulation, thereby polluting the broader information ecosystem.

Information laundering is particularly dangerous in democratic societies, where openness and free expression make the public sphere more permeable to repeated, disguised falsehoods. By embedding disinformation within seemingly legitimate discourse, malign actors exploit the very transparency that underpins liberal democratic debate.

Malign actors exploit the very transparency that underpins liberal democratic debate

⁷ Pekka Kallioniemi, “[Russia Allegedly Spent \\$10 Million Funding US Media Company and its ‘Superspreader’ Creators](#),” *Byline Times*, 6 September 2024.

⁸ CPD, “Where the Kremlin Gets Money.”

⁹ Aleksandra Michałowska-Kubś, “[Coining lies. Kremlin spends 1.5 Billion per year to spread disinformation and propaganda](#),” *Debunk Disinformation Analysis Center*, 8 August 2022; Phil McCausland, “[Right-wing influencers say they were victims of alleged Russian plot](#),” *BBC*, 5 September 2024.

1.2.3. SOCIAL MEDIA SUPERSPREADERS

Authoritarian regimes, particularly the Russian Federation, have increasingly relied on social media ‘superspreaders’ to execute disinformation campaigns. These are high-reach individual accounts that amplify false

or misleading narratives, often under the guise of independent commentary. Initially prominent during the COVID-19 pandemic – with research showing that 65% of online health misinformation could be traced to just 12 accounts – this model has since migrated into geopolitical information warfare.¹⁰ Superspreaders are now instrumental in promoting pro-Kremlin narratives related to the Russo-Ukrainian war and other foreign policy issues.¹¹

Russian influence operations increasingly outsource propaganda to popular western figures with large followings

Rather than relying solely on state media or bot farms, Russian influence operations increasingly outsource propaganda to popular western figures with large followings. These influencers, motivated by political ideology or financial gain, serve as effective intermediaries for hostile messaging. A striking example is the Tenet Media case, in which nearly \$10 million was covertly funnelled from Russian state media (*RT*) to American right-wing influencers to produce and disseminate pro-Russian content.¹² These operations obfuscate the origin of the message, lending Kremlin propaganda a facade of organic western support.

Many superspreaders operate without formal ties to foreign governments but are nonetheless drawn into the disinformation economy. Platforms like X (formerly Twitter) financially reward engagement through ad revenue, subscriptions, and impression-based monetisation – even when content is misleading or harmful.¹³ The incentive structure encourages sensationalism and polarisation, creating a business model where falsehoods are not only tolerated

but profitable. Compounding this issue, content moderation has been weakened on key platforms, with X, for instance, dismantling its Trust and Safety Council and scaling back enforcement against disinformation.¹⁴

These dynamics pose serious risks to democratic societies. Disinformation campaigns that exploit superspreaders can evade detection, polarise electorates, and erode trust in democratic institutions – often without any visible foreign branding. As Lieutenant General HR McMaster observed, such operations are “designed to sow divisions in society, distort reality, and erode confidence in democratic principles.”¹⁵ Addressing

these threats requires not only understanding of how they operate, but also recognising the systemic vulnerabilities that enable their success.

1.3. ASYMMETRY IN THE INFORMATION WAR

The information conflict between authoritarian regimes and liberal democracies is fundamentally asymmetrical. While autocratic states like Russia and China maintain stringent control over their domestic information environments, liberal democracies uphold open and pluralistic media landscapes. This structural divergence creates a significant imbalance: authoritarian regimes are largely insulated from external narratives, whereas open societies are susceptible to foreign influence and disinformation campaigns.

Authoritarian regimes are largely insulated from external narratives

In authoritarian states, the domestic information space is treated as a strategic asset, subject to rigorous surveillance, censorship, and state orchestration. In Russia, the media landscape is dominated by state-owned or state-aligned outlets, and independent

¹⁰ Center for Countering Digital Hate, [The Disinformation Dozen. Why Platforms Must Act On Twelve Leading Online Anti-Vaxxers](#) (CCDH, 2021); Shannon Bond, [“Just 12 People Are Behind Most Vaccine Hoaxes on Social Media, Research Shows,”](#) *NPR*, 13 May 2021.

¹¹ Matthew R. DeVerna et al, [“Identifying and Characterizing Superspreaders of Low-Credibility Content on Twitter,”](#) *Plos One* 19, no. 5 (22 May 2024).

¹² DOJ, “DOJ Disrupts Russian Influence;” Kallioniemi, “Russia Allegedly Spent \$10 Million.”

¹³ Carlos Diaz Ruiz, [“Disinformation on digital media platforms: A market-shaping approach,”](#) *New Media & Society*, 27(4): 2188-2211.

¹⁴ Thomas Brewster, [“Elon Musk Fired 80% of Twitter/X Engineers Working on Trust and Safety,”](#) *Forbes*, 10 January 2024; Siladitya Ray, [“Twitter Shuts Down Its Trust and Safety Council – Here’s What You Need to Know,”](#) *Forbes*, 13 December 2022.

¹⁵ Tatham, *Information Operations*.

journalism faces constant repression. Internet access is filtered through national systems like Russia's 'sovereign internet' infrastructure, which enables the government to throttle or block undesirable content at will. Platforms such as YouTube, Facebook, and independent news websites have been banned or restricted, particularly during periods of political sensitivity.

China presents an even more controlled model. Its Great Firewall functions as both a technological and political barrier to foreign information. Western platforms like Google, Twitter, and Wikipedia are inaccessible without circumvention tools, and domestic platforms are subject to real-time censorship, keyword filtering, and algorithmic controls. The Chinese Communist Party maintains an extensive propaganda apparatus, including 'opinion guidance' teams and cyber units tasked with shaping online discourse and neutralising dissent. Any foreign effort to inject factual or critical information into the Chinese media ecosystem faces near-immediate suppression.

These closed information environments make offensive information operations against authoritarian regimes exceptionally difficult. Attempts to reach Russian or Chinese audiences with independent journalism, human rights reporting, or alternative geopolitical perspectives are routinely blocked, removed, or drowned out by state propaganda. In rare cases where such content breaks through, authorities can swiftly identify and eliminate the source, often with legal or technological force. The result is a lopsided information battlefield where autocracies are protected by digital firewalls while simultaneously projecting influence outward.

In contrast, liberal democracies uphold a commitment to free and open communication, even in the face of manipulation. This openness is a democratic strength – but also a security vulnerability. Social media platforms in the west serve as conduits for hostile narratives, conspiracy theories, and propaganda, often originating from authoritarian actors. These campaigns exploit algorithmic amplification, anonymous accounts, and media fragmentation to undermine trust, inflame polarisation, and distort political discourse.

Because democracies prioritise freedom of expression, they have limited means to filter or suppress foreign content without provoking concerns over censorship or violating core democratic norms.

This asymmetry presents a strategic dilemma. While authoritarian regimes enjoy near-total control over their domestic narratives and immunity from counter-messaging, they can exploit the transparency and permissiveness of democratic systems to conduct large-scale influence operations with minimal resistance.

Democracies are perpetually on the defensive

This creates a situation in which democracies are perpetually on the defensive – monitoring, debunking, and reacting – while autocracies operate with impunity behind fortified digital borders.

To summarise, the global information environment is inherently unbalanced:

- **Authoritarian regimes** enjoy near-total control over what their citizens see, making them impervious to external counter-narratives.
- **Democratic societies** remain open and vulnerable, unable to restrict harmful content without raising legitimate concerns about censorship and free speech.

2. UNEVEN BATTLEGROUND: DISPARITIES IN DISINFORMATION FUNDING

The strategic contest over information integrity is marked by a significant imbalance in resource allocation. Authoritarian states, notably Russia and China, commit substantial financial resources to state-controlled media and influence operations. In contrast, liberal democracies, including the European Union, allocate comparatively modest budgets to counteract disinformation, reflecting differing governance structures and budgetary priorities.

2.1. AUTHORITARIAN INVESTMENT IN PROPAGANDA

Authoritarian regimes have institutionalised disinformation as a core component of their foreign and domestic policy strategies. Russia, for instance, has significantly increased its investment in state media and propaganda. According to the Ukrainian Ministry of Culture and Information Policy, Russia allocated over \$1.5 bn to propaganda efforts in 2023, with plans to increase this to \$1.8 bn in 2024, representing more than 0.1% of its GDP.¹⁶ This includes funding for *RT*, *Sputnik*, and other platforms that broadcast Kremlin-aligned narratives globally.

Authoritarian regimes have institutionalised disinformation as a core component of their foreign and domestic policy strategies

Moreover, covert operations – such as payments to western influencers via intermediaries – are funded through additional opaque budget lines and state-linked enterprises.¹⁷ These mechanisms allow Russia to sustain both domestic control and foreign influence campaigns at scale.

China's media influence strategy is equally extensive. Though official numbers are harder to verify, estimates suggest billions are spent annually on global information expansion through *CGTN*, *Xinhua*, and Belt and Road media initiatives.¹⁸ Like Russia, China leverages centralised state control and censorship to shape narratives both at home and abroad.

2.2. COLLABORATIVE NARRATIVE ECOSYSTEMS

Beyond their individual disinformation efforts, Russia and China increasingly collaborate in the information domain, forming a de facto authoritarian narrative ecosystem. While their strategic goals may differ, both regimes share a vested interest in undermining liberal

democratic norms, promoting multipolarity, and discrediting western institutions.¹⁹ This convergence is most visible in their coordinated messaging on topics such as NATO expansion, US foreign policy, the Ukraine war, and the legitimacy of liberal democracy.

Russia and China increasingly collaborate in the information domain, forming a de facto authoritarian narrative ecosystem

State media outlets like *RT* and *CGTN* often amplify each other's content, especially when it serves shared geopolitical interests – for instance, framing the west as hypocritical, decadent, or in decline. In the global south and in emerging markets, both states push narratives that challenge western development models and elevate their own governance systems as stable alternatives. China, in particular, has built an extensive media infrastructure across Africa, including content-sharing agreements, journalist training programmes, and co-branded news production with local outlets, allowing Beijing to shape information flows and frame public discourse. Russia, by contrast, relies more heavily on direct propaganda distribution through outlets like *Sputnik* and *RT*, establishing a presence in African broadcast ecosystems by providing cheap or free content to cash-strapped local stations. In South America, *RT* has become one of the most widely consumed international news sources, often perceived as a legitimate counterweight to western outlets and compared in popularity to the *BBC* in Europe.

Furthermore, Russia and China engage in joint media training programmes, co-host summits on 'information sovereignty', and share best practices for censorship, surveillance, and online influence. This strategic alignment magnifies the reach and credibility of their messaging, creating a reinforcing loop of anti-western content that exploits the open media environments of liberal democracies. Such coordination underscores the need for democratic states to view disinformation not

¹⁶ Filter, "How Much Does Russia Spend on Propaganda?"; Michałowska-Kubś, "Coining lies."

¹⁷ CPD, "Where the Kremlin Gets Money."

¹⁸ Artemchuk, "Russia to Increase State Propaganda Spending."

¹⁹ For example, see: Jerker Hellström, Matti Puranen, Santeri Kytöneva, and Pekka Kallioniemi, [Are Russian Narratives Amplified by PRC Media? A Case Study on Narratives Related to Sweden's and Finland's NATO Applications](#) (NATO StratCom, 2024).

merely as isolated campaigns, but as part of a shared authoritarian playbook designed for long-term ideological competition.

Coordination underscores the need for democratic states to view disinformation as part of a shared authoritarian playbook designed for long-term ideological competition

2.3. EU'S COUNTER-DISINFORMATION FUNDING

The EU has made efforts to build societal resilience and improve media literacy, but these efforts remain underfunded relative to the scale of the threat:

- **European Digital Media Observatory (EDMO):** In 2022, the European Media and Information Fund (EMIF) awarded €5.7 mn to 33 anti-disinformation projects across 21 countries, while the total requested funding was €19.4 mn – more than triple the amount available.²⁰
- **Horizon Europe projects:** In 2024, the EU allocated €7.3 mn to projects such as Vital Intelligence to Investigate Illegal Disinformation (VIGILANT) and Fake News Risk Mitigator (FERMI) to support law enforcement and civil society in identifying and countering disinformation ahead of elections.²¹
- **Media literacy programmes:** In 2025, nearly €5 mn was made available through EU calls for proposals aimed at strengthening critical media literacy skills and public awareness about disinformation.²²

These investments, while valuable, fall far short of matching the scope and pace of authoritarian propaganda campaigns.

²⁰ Florence School of Transnational Governance, “[EMIF awards €5.7M for projects fighting disinformation in 2022](#),” European University Institute, 3 November 2022.

²¹ Directorate-General for Migration and Home Affairs, “[Research projects help combat disinformation ahead of elections](#),” European Commission, 30 May 2024.

²² European Commission, “[EU funding of €5 million to strengthen media literacy and resilience to disinformation](#),” 30 April 2025.

2.4. STRUCTURAL CONSTRAINTS IN LIBERAL DEMOCRACIES

Liberal democracies face inherent constraints when addressing disinformation:

- **Budgetary scrutiny:** Any significant investment in counter-disinformation efforts requires public justification, parliamentary debate, and transparency – all of which slow down resource allocation and may provoke partisan controversy.
- **Freedom of expression:** Legal and normative protections for free speech limit the capacity of democratic governments to regulate or remove even demonstrably harmful content, especially on privately owned platforms.
- **Decentralised media ecosystem:** The diversity of outlets and lack of centralised control make it difficult to coordinate a unified response across jurisdictions or sectors.

3. THE US VARIABLE: A STRATEGIC UNCERTAINTY

In recent years, Russia has found a potent and willing ally in the MAGA movement in the United States – a populist-nationalist force that shares the Kremlin’s disdain for multilateral institutions, NATO, and the European Union. This convergence represents a strategic evolution in Russia’s approach: rather than merely opposing the west externally, the Kremlin now actively cultivates domestic allies within western societies to undermine liberal democratic norms from the inside.

The ideological alignment is striking. Russian state media and MAGA-aligned figures often mirror each other’s narratives on issues such as NATO expansion, the war in Ukraine, ‘globalist elites’, election integrity, and cultural degeneration in the west. The Kremlin’s firehose of falsehood propaganda model has been especially effective in disseminating these narratives through both state-owned

channels and social media influencers embedded within the MAGA movement. Russia no longer needs to fabricate western voices – it simply funds or amplifies those already willing to echo its themes.

Russia no longer needs to fabricate western voices – it simply funds or amplifies those already willing to echo its themes

This strategy was publicly exposed in the *Tenet Media* case. In 2024, the US Department of Justice indicted two individuals for laundering nearly \$10 mn from the Russian state broadcaster *RT* to finance a Tennessee-based media operation that employed prominent MAGA-affiliated influencers. These figures were paid up to \$400 000 per month to produce pro-Kremlin content aimed at US audiences, attacking Ukraine, praising Russian leadership, and sowing distrust in western institutions.²³ By laundering the funding through shell companies and fake personas, the Kremlin cloaked foreign propaganda in the voice of American conservatism.

The lines between Russian and Chinese influence efforts are increasingly blurred

While Russia has been the primary driver of such covert influence operations, it is not acting alone. A growing body of evidence suggests China is engaging in similar tactics, targeting far-right political actors in Europe to subtly reshape public discourse. In one striking case reported by *Le Monde* in 2023, Chinese intelligence operatives were found directing a European far-right politician to promote pro-Beijing narratives, criticise NATO, and denigrate the US – mirroring Kremlin objectives but through a different strategic lens.²⁴ The lines between Russian and Chinese influence efforts are increasingly blurred, with both regimes seeking to exploit polarisation, populism, and distrust in democratic governance to destabilise the west.

The impact of these operations is most acutely felt in Europe, but the transatlantic relationship is not monolithic. While MAGA-aligned leadership now holds power in Washington, US foreign policy remains a complex and sometimes contradictory apparatus. Key institutions – including the intelligence community, elements of the Pentagon, and US diplomatic channels – continue to provide meaningful support to European allies and Ukraine. Intelligence sharing, military assistance, and cyber defence cooperation remain active. However, the decision-making environment within the Trump administration is notably volatile, marked by rapid shifts in tone and direction, especially from the President himself. Policy reversals, conflicting statements, and leadership turnover have made it difficult for international partners to anticipate long-term US positions.

This unpredictability underscores a strategic vulnerability: while some parts of the US government remain committed to countering foreign influence and supporting European security, others may obstruct, downplay, or reverse those efforts based on short-term political calculations or ideological alignment.

Compounding the issue, terms such as disinformation and foreign influence (FIMI) have become politically radioactive in Washington. Once considered essential to national security, these issues are now frequently dismissed by MAGA-aligned figures as partisan smears or tools of censorship. The Trump administration has systematically defunded and deactivated programmes designed to track and counter foreign information operations, including components of the State Department's Global Engagement Center (GEC) and Homeland Security's disinformation monitoring teams. In parts of Congress and conservative media, disinformation is no longer seen as a threat – it is seen as a talking point for opponents.

²³ DOJ, "DOJ Disrupts Russian Influence;" Kallioniemi, "Russia Allegedly Spent \$10 Million."

²⁴ "[Chinese Spies Recruited Far-Right Belgian Politician as Intelligence Asset](#)," *Le Monde*, 15 December 2023.

CONCLUSION AND RECOMMENDATIONS

The information war is not a future threat – it is the defining battlefield of the present. Authoritarian regimes are using narrative

abstain from mimicking authoritarian control when the strategic posture in the information domain is rethought. The application of defensive tools needs to be supported by active defence of the information integrity and the freedom of expression, which cannot be passively assumed.

The information war is not a future threat – it is the defining battlefield of the present

ESTABLISHMENT OF STRATEGIC AUTONOMY IN THE INFORMATION SPACE

control, psychological operations, and digital manipulation not only to protect their regimes but to destabilise and divide the democratic world. The west cannot afford to treat this as a marginal or soft-security issue. It must recognise information dominance as a core pillar of modern statecraft.

The ideological overlap between authoritarian regimes and rising illiberal forces within the west presents a long-term challenge that cannot be outsourced or deferred. In the face of this development, Europe cannot afford to treat the US as a consistently reliable partner in the fight against authoritarian information warfare. While the transatlantic co-operation remains valuable, it cannot be assumed as stable. Therefore, the fight against foreign influence operations must be coordinated, sustained, and, where necessary, led independently of Washington's shifting political winds.

The west must recognise information dominance as a core pillar of modern statecraft

This paper has examined how structural asymmetries – in decision-making, funding, and narrative control – have given actors like Russia and China a significant head start. But this imbalance is not irreversible. With sufficient political will, strategic investment, and agile execution, democracies can turn the tide.

To address this uncertainty, Europe must build strategic redundancy into its information defence posture through the following means:

Having outlined the strategic advantages and tools employed by authoritarian regimes, the next section proposes concrete actions the west must take to reclaim initiative and assert democratic values in the information domain.

Europe cannot afford to treat the US as a consistently reliable partner in the fight against authoritarian information warfare

ACKNOWLEDGEMENT OF THE FUNDAMENTAL STRUCTURAL DIFFERENCES IN THE INFORMATION ECOSYSTEMS

The level of control that authoritarian regimes have over their information ecosystems differs significantly from the abilities of liberal democracies. When taking this aspect into consideration, it becomes visible that vital defensive tools like fact-checking, media literacy, and platform regulation are insufficient on their own. However, it is necessary to

- Expanding intra-EU threat intelligence coordination and crisis communication capabilities;
- Deepening bilateral ties with reliable democratic partners such as Canada, the UK, South Korea, Taiwan, and Japan;
- Strengthening EU-NATO StratCom collaboration in ways that do not rely on US executive leadership;
- Investing in autonomous monitoring, narrative disruption, and digital infrastructure to sustain resilience regardless of political shifts in Washington.

STRATEGIC SPENDING IN THE INFORMATION WAR

The disparity in funding present in the realm of information warfare underscores a strategic vulnerability. While authoritarian states can swiftly mobilise substantial resources to propagate their narratives, liberal democracies must navigate complex political and ethical landscapes to mount effective countermeasures. In addition to that, the information domain was treated – particularly within the EU – as an auxiliary concern, resulting only in a fractional annual funding of counter-disinformation initiatives compared to the efforts of adversarial states. This discrepancy results in a permanent state of reactive posture, where authoritarian regimes dictate the tempo, topics, and tone of global conversations.

- To close the funding gap, Europe and its allies must elevate counter-disinformation spending to levels that reflect the scale of the threat, institutionalise budget lines, and treat information resilience as a core infrastructure investment.
 - At the EU level, a dedicated Information Security Fund could be established within the Multiannual Financial Framework (MFF), with clear targets for supporting open-source intelligence (OSINT) initiatives, media literacy, and strategic communication.
 - National governments should similarly embed counter-disinformation spending within defence and education ministries, with annual reporting to parliaments to ensure transparency and cross-party legitimacy.
 - At the NATO level, the eligible defence contributions need to be expanded to include investments in information operations. The inclusion of multilingual pre-bunking campaigns, threat monitoring infrastructure, and rapid-response communications would incentivise member states to scale efforts proportionate to the threat.

- Finally, it is required that, next to increased investments, the resilience against disinformation is enhanced as well through innovative approaches that respect democratic values.

PRE-BUNKING AS A STRATEGIC DEFENCE LAYER

The proactive exposure of disinformation tactics and narratives, known as pre-bunking, enables citizens to recognise and reject manipulative content in real time. To engage disinformation before it gains traction can be remarkably effective, as research in behavioural science and cognitive psychology shows.

- Therefore, pre-bunking must become a core component of national and EU-level information security strategies through a coordinated governance structure that avoids bureaucratic bottlenecks.
- The EU should expand their Strategic Communications Taskforce under the European External Action Service (EEAS) with a dual mission: (1) to coordinate cross-border campaigns and (2) to act as a central distribution node for OSINT, civil society findings, and narrative monitoring. This task force would work alongside EDMO and NATO's Strategic Communications Centre of Excellence (StratCom COE) but maintain direct lines to the European Commission's crisis management mechanisms.
- National governments should create information resilience units within their ministries of interior or foreign affairs, equipped with rapid procurement authority, standing partnerships with tech platforms, and embedded liaisons to civil society actors. These units should maintain multilingual content pipelines and crisis playbooks ready for deployment ahead of elections, protests, or geopolitical shocks.

But to be effective, it is necessary that pre-bunking occurs where the people are – on YouTube, TikTok, Instagram, in schools, on gaming platforms, and in popular television formats, which can be implemented through the following measures:

- **Integrate pre-bunking into education systems:** Media literacy and critical thinking curricula should include modules that teach how disinformation works and how to spot it. This is particularly urgent at the secondary school level, where young people are first exposed to politicised social media environments.
- **Launch EU-wide public awareness campaigns:** Use television, YouTube, TikTok, and other mass-reach platforms to roll out recurring, engaging content that explains disinformation tactics and highlights common narratives used by foreign actors – especially Russian and Chinese sources.
- **Deploy strategic pre-bunking around known flashpoints:** Elections, protests, and crises are consistently targeted by hostile information operations. Pre-bunking should be timed in advance of these events to reduce societal vulnerability.
- **Coordinate through EDMO and NATO COEs:** DMO, in partnership with NATO Strat-Com, should coordinate member states' pre-bunking strategies, pool research, and distribute effective content templates and behavioural insights.
- **Fund experimental campaigns:** Support agile civil society teams and academic institutions to experiment with tone, medium, and delivery of pre-bunking content. What works in Estonia might not work in France or Italy – localised, adaptive messaging is key.

BUILDING AN INTELLIGENCE-LED MONITORING CAPABILITY

Since prevention begins with visibility, liberal democracies cannot afford to monitor disinformation threats passively or sporadically in today's fast-moving information environment.

- Therefore, active, continuous, and intelligence-led monitoring of hostile information operations must become a strategic priority.

- To catch up to authoritarian regimes, a hybrid monitoring system is needed to blend technological scale with human expertise.

To establish such a system, it is necessary to move beyond fragmented, academic, or reactive research towards investment in permanent monitoring infrastructures, which consist of:

- AI-powered analytics to scan millions of data points across languages and platforms;
- Expert OSINT investigators capable of identifying patterns and attribution;
- Political scientists, linguists, and regional experts to interpret context and intent;
- Strategic foresight teams to anticipate where campaigns may emerge or evolve next.

Monitoring must not only detect disinformation once it spreads. It must focus on upstream intelligence: identifying incubation points in closed Telegram groups, fringe video platforms, domestic channels in Russia and China, and diaspora communities vulnerable to influence. This means placing more emphasis on foreign-language monitoring and non-western digital ecosystems, which are often overlooked by conventional approaches.

A set of strategic priorities is recommended for the implementation:

- **Create national information monitoring centres:** Each member state should develop a centralised node for cross-agency threat tracking – linked into an EU-wide or NATO-coordinated fusion hub.
- **Support OSINT ecosystems:** Invest in trusted independent OSINT actors that can respond quickly and flexibly to emerging campaigns and serve as public-facing validators of state findings.
- **Integrate monitoring with cyber defence and intelligence agencies:** Information threats must be treated with the same urgency as cyberattacks, requiring seamless coordination across technical, diplomatic, and security structures.

- **Build partnerships with tech platforms:** While independence must be protected, structured collaboration with social media platforms can allow governments to better identify viral disinformation and understand algorithmic amplification mechanisms.

KEY OFFENSIVE AVENUES

Authoritarian states are not merely spreading disinformation – they are conducting coordinated information offensives designed to destabilise democratic systems, fracture alliances, and demoralise populations. If liberal democracies fail to go on the offensive, they will continue to cede the initiative – and with it, the information battlefield itself. In other words, we are at war. Therefore, the west must now begin to identify and engage with the vulnerabilities of authoritarian regimes.

Strategic communication must evolve from passive rebuttal to targeted disruption

These regimes are not monoliths. They are deeply fragile in many areas: economically brittle, demographically strained, socially unequal, and reliant on narrative control for political survival. Strategic communication must evolve from passive rebuttal to targeted disruption, for which it can follow these key offensive avenues:

- **Exploit authoritarian weaknesses:** Russia faces mounting demographic collapse, brain drain, elite corruption, regional inequality, and growing disillusionment among younger generations. China wrestles with youth unemployment, internal censorship backlash, and elite factionalism. These fault lines offer entry points for carefully targeted narrative disruption.
- **Understand and penetrate their information ecosystems:** Effective offensives begin with a deep understanding. Western institutions need to invest in long-term studies of authoritarian digital cultures – how narratives form, how platforms are used, and where internal dissent is percolating. Western actors must develop greater fluency in platforms like WeChat, VK, RuTube, Telegram, and TikTok and craft native, regionally contextualised influence efforts.
- **Create strategic content for adversary audiences:** Messaging should be tailored to specific societal fissures: economic mismanagement, military casualties, internal repression, elite hypocrisy. This requires multilingual, culturally sensitive teams capable of developing content that resonates with disaffected populations – not western talking points, but targeted narratives that exploit existing grievances.
- **Deploy agile units for offensive information operations:** Borrowing from the military concept of special operations forces, governments should support small, high-capability digital teams with the freedom to act flexibly. These units can experiment with meme warfare, counter-messaging, satire, and localised content – using open-source tools and adaptive tactics to seed doubt and challenge regime narratives.
- **Leverage influencers and diaspora voices:** Authoritarian regimes fear nothing more than dissent from within. Platforms should amplify independent journalists, artists, cultural figures, and defectors who can authentically question state narratives from the inside. These individuals have greater credibility and reach than formal state messaging, and can shift perceptions organically over time.
- **Study and learn from Navalny's Anti-Corruption Foundation (FBK):** One of the most successful examples of strategic information disruption comes from inside Russia itself. Navalny's FBK used social media, YouTube documentaries, and viral investigative journalism to expose Kremlin corruption at the highest levels – including the now-infamous documentary on "Putin's Palace," which has garnered over 120 million views. Their work forced the regime to react, defend, and repress – proving that targeted, emotionally resonant, fact-based campaigns can deeply unsettle even tightly controlled authoritarian systems. Despite brutal repression, FBK continues to operate in exile, showing that asymmetric information power is still within reach.

- **Integrate disruption into broader foreign policy:** Offensive information operations should be coordinated with diplomatic, economic, and security strategies. For example, messaging on Kremlin elite corruption should align with sanctions policy; narratives about People’s Liberation Army (PLA) overreach should support Indo-Pacific deterrence objectives.

ETHICAL BOUNDARIES FOR OFFENSIVE INFORMATION OPERATIONS

Offensive strategies in the information domain must be grounded in the values that liberal democracies seek to defend. The objective is not regime change, social destabilisation, or manipulation mirroring authoritarian tactics. Rather, the aim is strategic narrative disruption: the deliberate, truth-based exposure of authoritarian corruption, repression, and hypocrisy in ways that empower local dissent, inform global audiences, and weaken the adversary’s ability to control its own narrative.

Offensive strategies in the information domain must be grounded in the values that liberal democracies seek to defend

- **First and foremost, all content disseminated as part of offensive operations must be truthful, evidence-based, and verifiable.** Democracies cannot afford to compromise on credibility, even for tactical gain. Fabricated stories risk eroding public trust and playing directly into the hands of adversaries who thrive on claims of western hypocrisy.
- **Second, offensive messaging must be designed with cultural fluency and contextual sensitivity.** Content aimed at authoritarian audiences should reflect a deep understanding of local languages, histories, grievances, and socio-political dynamics. Western actors must resist the impulse to project their own values in a one-size-fits-all format. Instead, messaging should amplify voices and issues that already exist within target societies – whether those are tied to corruption, elite privilege, generational tensions, or state

violence. The goal is not to impose an external narrative, but to surface internal contradictions and support indigenous critique.

- **Third, offensive operations must be subject to clear legal oversight and institutional accountability.** These efforts, while flexible and creative, cannot be left entirely to informal networks or opaque agencies. Democratic governments should establish oversight mechanisms – such as parliamentary committees or independent review panels – to evaluate the legality, proportionality, and potential unintended consequences of offensive campaigns. Where possible, independent ‘red teams’ should assess operations in advance, simulating adversary responses and identifying risks of escalation or blowback.

By operating within these ethical boundaries, democracies can differentiate themselves from the authoritarian regimes they seek to challenge. Transparency, restraint, and fidelity to truth are not constraints – they are the qualities that give democratic information strategies both their moral legitimacy and their strategic durability. In a contest over credibility and trust, it is not enough to out-shout the adversary.

The west must lead by example – and win by being better, not simply louder. By modelling transparency and restraint, democracies can differentiate themselves from authoritarian information warfare while still taking the initiative.

ENGAGING CIVIL SOCIETY AS FORCE MULTIPLIERS

Governments cannot win the information war alone. The most effective responses to disinformation and authoritarian influence have often come not from state institutions, but from small, agile, and independent civil society actors – open-source investigators, cultural creators, media literacy NGOs, and digital activists. These groups operate with speed, adaptability, and credibility that state structures often lack. In the age of decentralised propaganda, decentralised

countermeasures are not a luxury – they are essential.

Authoritarian states fear organic civil movements because they represent precisely what their systems suppress: autonomous, truth-driven, horizontally networked actors. Whether it is investigative platforms like *Bellingcat*, satire and monitoring accounts like *Vatnik Soup*, or activist collectives like Navalny's FBK, civil society is already on the frontlines – often with minimal institutional support.

- **Fund with flexibility:** Governments and international institutions must create light-touch, rapid-access funding mechanisms for civil actors in the information space. Bureaucratic grant programmes with 12-month review cycles are incompatible with a real-time media war.
- **Protect and elevate credible voices:** Journalists, whistle-blowers, and researchers exposing hostile influence operations are increasingly targeted by harassment, legal intimidation, and digital attacks. Democracies must not only fund their work but actively shield them from retaliation.
- **Institutionalise collaboration without control:** Governments should act as conveners, not commanders. Structures like public-private task forces, hybrid labs, and protected data-sharing platforms can support civil society without compromising its autonomy or credibility.

PLANNING ACROSS TIME HORIZONS TO BUILD SUSTAINABLE INFORMATION RESILIENCE

The stated solutions must be structured across short-, medium-, and long-term timelines. In the short term, governments can build rapid-response capabilities and fund offensive countermeasures.

- **Short-term (0–18 months) rapid disruption and defence:**
 - Expand pre-bunking and real-time counter-messaging capacity;

- Fund offensive narrative initiatives and civil society and activist organisations targeting adversary vulnerabilities;
- Scale up OSINT partnerships and monitoring units;
- Prepare strategic communication plans for key flashpoints (e.g., elections, crises).

In the medium term, strategic communication hubs and public-private platforms can increase narrative resilience.

• Mid-term (2–5 years) institutional and infrastructure growth:

- Establish national information resilience centres;
- Embed disinformation threat intelligence in defence and diplomacy;
- Reform public broadcasting and digital education mandates;
- Invest in secure digital platforms with democratic content priorities.

In the long term, educational reforms must focus on critical media literacy to build durable cognitive immunity to manipulation.

• Long-term (5–15 years) building cognitive immunity:

- Integrate critical media literacy into core education curricula;
- Train future educators, journalists, and civil servants in information security;
- Promote democratic digital culture through art, storytelling, and youth media.

In summary, the west cannot afford to remain reactive. The information war will be won not only by defending our values, but by strategically projecting them into contested information environments. The next chapter of this conflict must be one of initiative, coherence, and sustained ambition. It is about reasserting the strategic and moral leadership of democratic societies in the 21st century. To win this war, we must take back the initiative and start setting the agenda again.

RECENT ICDS PUBLICATIONS

REPORTS

- Gretskiy, Igor. *Not Quite Agents of Change: Russian Anti-War Grassroots Initiatives in Europe*. October 2025.
- Blockmans, Steven, Butrint Berisha. *From Stalemate to Solution: Rethinking EU Approaches to Bilateral Disputes in the Context of Enlargement*, October 2025.
- Hosaka, Sanshiro, Toomas Hanso. *Between Giants: Central Asia Balancing China, Russia, and the Rest*. September 2025.
- Jermalavičius, Tomas, Henry Rõigas, Oleksandr Sukhodolia, and Dmitri Teperik. *The Staying Power of Ukrainian Lights. Lessons of Wartime Resilience of the Electricity Sector*. May 2025.
- Arjakas, Merili, Kai Kaarelson, Solveig Niitra, Hille Hanso, Ivan U.K. Lyszcz. *Eesti roll muutuvus rahvusvahelise arengukoostöö arhitektuuris* [Estonia's Role In the Changing Architecture of International Development Cooperation]. March 2025.
- Klyszcz, Ivan U.K., Tony Lawrence, Eric Chan, Jyun-yi Lee. *Deterrence and Hybrid Warfare: Lessons from Russia's War in Ukraine for Taiwan and the Nordic-Baltic Region*. February 2025.
- Hosaka, Sanshiro. *A Mountain to Climb: Russia's Influence in the South Caucasus and EU Policy Options*. January 2025.

POLICY PAPERS

- Hall, Eric. *Europe's Forthcoming Sahel Strategy: A Limited Role in a Multipolar Region*." October 2025.
- Lawrence, Tony, Niklas Granholm, Björn Ottosson, and Igor Schvede. *Hybrid and High-End Warfare in the Baltic Sea Region: Safeguarding our Maritime Domain*." September 2025.
- Alatalu, Siim. *Cyber Solidarity in the Making: Is the EU Stepping into NATO's Blind Spot?*" August 2025.
- Lawrence, Tony, Felix Gasper, and Dick Zandee. *Defending Europe's Skies: Challenges and Prospects*." May 2025.
- Klyszcz, Ivan U.K. *Distance is Not a Shield. Russia's Transnational Repression in Wartime*," May 2025.
- Praks, Henrik. *Russia's Hybrid Attacks in Europe: From Deterrence to Attribution to Response*." April 2025.

ANALYSES

- Mikelsaar, Anniki. *Ruptures at the Top of the World: High North Network Infrastructure Protection*." September 2025.
- Gasper, Felix, Lukas Mugele. *Forward Defence in the Cold War*." August 2025.
- Leveque, Arthur, and Justin Leveque. *Foreign Interference in Distant Territories: French Territories on Azerbaijan's, Russia's, and China's radars*." August 2025.
- Larsen, Henrik. *Toward a Europeanised NATO*." June 2025.
- Hanso, Toomas. *Central Asia's New Railways: Russia's Pain, China's Gain*." March 2025.
- Alatalu, Siim. *The EU's NIS2 Directive A Business Opportunity for the Defence Sector*." March 2025.

BRIEFS

- Heap, Ben, Sahaidachnyi Security Center, Hennadiy Maksak, and Laurynas Jonavičius. *Russia's War in Ukraine Series*. October 2025.
- Klyszcz, Ivan U. K., *Russia and the Red Sea since 2022: Militarised Foreign Policy or Strategy of Conflict?*." September 2025.
- Nazarov, Mykola. *Ukrainian War Refugees in Estonia: Sociodemographic Portrait and Support Policies*." September 2025.
- Hosaka, Sanshiro. *Trump-Brokered Azerbaijan-Armenia Peace Deal: Breakthrough or Another Geopolitical Conundrum?*" August 2025.
- Kimoita, Stephen. *Kenya's Foreign Policy Towards Europe and Estonia*." July 2025.



ICDS.TALLINN



@ICDS-TALLINN.BSKY.SOCIAL



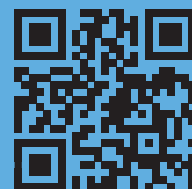
@ICDS _ TALLINN



ICDS-TALLINN



WWW.ICDS.EE



INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
63/4 NARVA RD., 10120 TALLINN, ESTONIA
INFO@ICDS.EE

ISSN 2228-2068