POLICY PAPER:

THE CALM BEFORE THE STORM: STRATEGIC COMMUNICATION AND SYSTEMIC READINESS IN HYBRID CONFLICT

AUTHORS

Veronika Víchová	CENTER FOR AN INFORMED SOCIETY
Andrea Michalcová	CENTER FOR AN INFORMED SOCIETY

CENTER FOR
AN INFORMED
SOCIETY

The Center for an Informed Society (CIS) is a non-governmental, non-profit organization that is not affiliated with any political party. Our vision is a resilient and prepared Czechia against hybrid and authoritarian influence.

www.informedsociety.cz

CENTER FOR AN INFORMED SOCIETY

This policy paper has been prepared with the support of the **British Embassy Prague**.

www.gov.uk/world/organisations/british-embassy-prague

British Embassy Prague

The policy paper has been prepared based on the conclusions of the Resilient Europe 2025 conference, co-organized with the **Ministry of Foreign Affairs of the Czech Republic**.

mzv.gov.cz

Ministry of Foreign Affairs of the Czech Republic

INTRODUCTION

Hybrid threats, including disinformation, cyberattacks, foreign influence operations, and covert funding, have become persistent and adaptive challenges for European democracies. These threats exploit vulnerabilities in political systems, public trust, digital infrastructure, and societal cohesion. This policy papers draws on insights from the **Resilient Europe 2025 conference, which was held in Prague in May 2025**[1], and the expertise of over 200 experts from 26 countries attending the conference discussion panels and side sessions. It outlines the evolving nature of hybrid threats, highlights practical responses adopted across Europe, and offers concrete recommendations for European leaders and state institutions aiming at improving resilience through legislation, communication, civil-military coordination, and digital regulation.

1 More information about the conference: https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/second_annual_international_conference.html

1. TRENDS IN HYBRID THREATS: EVOLVING TACTICS AND TOOLS

1.1 FROM DISINFORMATION TO NARRATIVE WARFARE

Hybrid influence campaigns no longer rely on isolated incidents of disinformation. Instead, they are sustained efforts to shift societal narratives, undermine democratic legitimacy, and manipulate historical memory. Russian operations in Moldova and Lithuania illustrate how **narratives can be tailored to target a nation's identity, history, and geopolitical orientation.** Examples include fabricated accusations of "Russophobia" when Moldova memorialized victims of Soviet deportations[2] or the dissemination of pro-Kremlin versions of Lithuanian history promoted by Russian officials[3]. These tactics aim to shape long-term public perceptions and polarize domestic debates.[4]

1.2 WEAPONIZATION OF TECHNOLOGY

Advanced technologies have amplified hybrid operations.

- **AI and deepfakes** are used to simulate real-time political developments. Ukraine's counter-response. President Zelenskyy's personal rebuttal and the viral "Ya tut" campaign demonstrated the value of authenticity.[5]
- **Algorithmic Manipulation:** Romania experienced coordinated manipulation of platform algorithms during the electoral period, targeting younger voters with anti-system messages.[6]
- **Encrypted and Decentralized Financing:** Moldova revealed Russia's use of crypto and informal cash networks to finance political destabilization. This was addressed via multi-agency cooperation involving financial regulators, customs, and intelligence services.[7]

1.3 DOMESTIC PROXIES AND EMBEDDED INFLUENCE

The line between foreign and domestic threats is increasingly blurred. Russia and other actors use **local politicians, businessmen, influencers, and media outlets** to advance disinformation or disrupt national policy. In Romania and Moldova, these proxies often receive covert financial support and echo Kremlin-aligned narratives under the guise of defending national sovereignty or traditional values. These actors are difficult to regulate and often operate legally, which complicates public attribution.

---

2 "Moldova Denies Soviet Deportation Exhibition as 'Russophobic'." Balkan Insight. https://balkaninsight.com/2023/07/14/moldova-denies-soviet-deportation-exhibition-is-russophobic/.

3 "Russia publishes a book on Lithuanian history, preface written by Lavrov" LRT. https://www.lrt.lt/en/news-in-english/19/2550706/russia-publishes-book-on-lithuanian-history-preface-written-by-lavrov.

4 You can find more information about narrative warfare here: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-28-moldovas-struggle-against-russias-hybrid-threats-from-countering-the-energy-leverage-to-becoming-more-sovereign-overall/

5 You can find more information about AI generated deepfakes here: https://www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18/

6 You can find more information about algorithmic manipulation here: https://www.rgsl.edu.lv/uploads/recent-publications-list/82/developing-legal-framework-for-resilient-society.pdf

7 "INTELLIGENCE REPORT EXPOSES RUSSIAN MEDDLING IN MOLDOVA'S EU VOTE." Vsquare. https://vsquare.org/intelligence-report-russian-meddling-in-moldova-eu-referendum-sis-ilian-sor/.

1.4 INFRASTRUCTURE SABOTAGE AND MARITIME THREATS

Hybrid tactics extend to **physical sabotage of critical infrastructure.** In the Baltic Sea, sabotage incidents have targeted internet cables and energy pipelines. “Shadow fleets” of unflagged or re-flagged vessels often operate undetected, exploiting international maritime law. Latvia and Estonia called for improved maritime situational awareness, legal reform, and joint EU-NATO monitoring operations. NATO’s Baltic Sentry mission is a notable example of multilateral response capacity.

2. BEST PRACTICES AND ACTIONABLE LESSONS

2.1 INSTITUTIONAL RESPONSES AND LEGAL INNOVATION

Moldova responded to hybrid pressure by launching a national cybersecurity agency, upgrading legislative frameworks, and **improving coordination among financial and intelligence institutions.** These measures helped prevent illicit funding during the 2024 elections and **shut down suspected foreign-financed operations.** For instance, Moldova stopped over €20 million in suspected illicit campaign financing linked to external actors. International cooperation with the U.S. Treasury and Europol was critical.[8]

Latvia's criminal code reforms allow **prosecution of AI-driven disinformation and coordinated foreign influence operations.** These laws provide a legal basis to act quickly during election periods and enable **cyber evidence** to be used in court proceedings - an innovation other EU members could adopt. Latvia also prioritizes regular meetings of its National Security Council and strong ties to military intelligence.[9]

Czechia created an MFA department dedicated to hybrid threats, which integrates policy on sanctions, cyber, and strategic communication. The department has also developed legal interpretations that balance procedural safeguards with operational efficiency, enabling Czech authorities to freeze assets linked to sanctioned actors without advance notice. Two court victories confirmed this new interpretation.

RECOMMENDATIONS:

- **Build resilient institutions by ensuring inter-ministerial mandates, legislative agility, and integration with civil society oversight.**
- **Encourage joint task forces that blend financial regulation, intelligence gathering, and legal enforcement.**

8 "EUPM Moldova: Moving forward towards sustainable security resilience in Moldova." EUPM. https://www.eeas.europa.eu/eupm-moldova/eupm-moldova-moving-forward-towards-sustainable-security-resilience-moldova_en.

9 "Parliament criminalises use of deep fakes that can influence elections." The Global State of Democracy Initiative. https://www.idea.int/democracytracker/report/latvia/may-2024.

2.2 ELECTORAL INTEGRITY AND TRANSPARENCY

Moldova created a **cross-institutional election protection task force.**[10] Key innovations include:

- Airport monitoring for illicit cash flows
- Real-time monitoring of campaign financing
- Civil society partnerships to report voter manipulation

Germany's experience with Storm-1516, a hybrid campaign linked to the Russian Internet Research Agency, revealed that even in the absence of technical interference, narrative manipulation can undermine confidence. Germany's Green Party was scapegoated for economic challenges through coordinated online campaigns. Authorities countered this by briefing journalists, engaging influencers, and rapidly debunking narratives using internal fact-checking.[11]

Romania's experience shows that resilience requires not only public education but raising the cost for adversaries. Their approach involves exposing financial links between domestic actors and foreign funders, legislative transparency, and persistent advocacy for platform accountability.[12]

RECOMMENDATIONS:

- **Election integrity requires year-round action.**
- **Establish multidisciplinary units to track disinformation, illicit financing, and threats to electoral commissions.**
- **Use public campaigns to raise awareness and strengthen voter confidence. State institutions should cooperate with relevant actors and amplifiers, including CSOs or influencers, to reach their target audiences with credible voices.**
- **Use the opportunities provided by the European Commission (including the Digital Services Act) to push on social media platforms, stress test your election process and other measures aimed at election protection ahead of time.**

10 "Combating Corruption in Political Finance." International IDEA. https://www.idea.int/sites/default/files/2025-04/combatting-corruption-in-political-finance.pdf.

11 "Germany warns of Russian disinformation targeting election." Reuters. https://www.reuters.com/world/europe/germany-warns-russian-disinformation-targeting-election-2025-02-21/.

12 "How Russia-backed influencers meddled in Romania's vote." Financial Times. https://www.ft.com/content/4b00e7ec-2c79-4313-b012-4f09f436f3ed.

2.3 STRATEGIC AND CRISIS COMMUNICATION

Countries such as Lithuania, Estonia, and Latvia have begun implementing systematic models that integrate government structures, crisis management, and technological innovation.

Lithuania launched a **national stratcom center in 2023, after 8 years of preparation.** It operates based on a threat index and close collaboration with the private sector. The private sector helps with detecting fake news and funding for NGOs. Public communication is governed by principles of speed and relevance.

Lithuania's National Crisis Management Center[13] runs **quarterly simulation exercises** and coordinates ministerial messaging through a rapid response unit. Their doctrine "If you don't respond quickly, you've accepted the narrative" is supported by **pre-approved content frameworks** and integrated communication teams.

Estonia has built a **networked evidence-based system and active media engagement.** However, it still struggles with slow publication of intelligence, even when the origin (e.g. Kremlin) is clear. Estonia institutionalized transparency by **proactively releasing responses to misinformation**, engaging domestic media, and facilitating media literacy training. During the 2018 Sputnik incident, the Ministry of Defence's immediate and comprehensive response became a regional model for proactive communication.

Ukraine has embraced platforms like TikTok and Telegram, investing in **young digital talent and NGOs to co-create content.** The blending of cultural resilience and civic messaging has helped maintain societal cohesion under fire.

Without **political acknowledgment of the seriousness** of hybrid threats, even the best-intentioned initiatives remain ineffective. Strategic communication often devolves into symbolic gestures, departments are created but lack real impact or authority. The key lesson from across the region is this: **no communication strategy can be effective unless it is anchored in a broader political framework** and backed by a genuine will to protect democratic institutions.

Strategic communication must stand outside ministers' political teams. It cannot be part of their cabinets, which are, by nature, political. Stratcom requires a professional, expert-driven, and long-term sustainable structure. It should be embedded within the public administration, specifically as part of the agenda focused on resilience against hybrid threats.

13 "Lithuania to establish National Crisis Management Centre." LRT. https://www.lrt.lt/en/news-in-english/19/1854923/lithuania-to-establish-national-crisis-management-centre.

RECOMMENDATIONS:

- Move from reactive to anticipatory communication.
- Equip strategic communication teams with behavioral insights, creative partnerships with CSOs and businesses, and multilingual content tools. Institutionalize best practices through training and shared playbooks, possibly also legislation.
- Political leadership must take responsibility for framing hybrid threats as a strategic priority and ensure adequate mandates, resources, and institutional backing for strategic communication agendas. However, strategic communication as such should not be conducted by political teams from the ministerial cabinets, but by professionals from the civil service without political agenda.
- Make sure the strategic communication teams and professionals have clearly given and transparent mandates, so that you can avoid uncertainty, paralysis, the spread of myths, or political backlash.
- Invest in systemic approaches that connect security analysis, communication experts, and crisis management.
- Transparency and credibility must be balanced with the protection of national security interests. Courage and confidence are key factors.

2.4 CIVIL-MILITARY AND CROSS-SECTORAL COOPERATION

Finland's total defense concept mandates **crisis preparedness in every sector**, including private logistics and regional health networks. Education and mandatory conscription include digital literacy and psychological resilience.

The Czech Republic's Armed Forces train soldiers in information hygiene and host simulations like Power of Hope, which prepares both military and civilian actors for hybrid crisis scenarios. The program emphasizes empathy, emotional regulation, and coordinated messaging.

Ukraine's Come Back Alive Foundation exemplifies embedded civil-military collaboration. Beyond equipment donations, it co-produces strategic communication and helps align parliament, civil society, and the armed forces.

RECOMMENDATIONS:

- **Make civil-military planning a routine feature of national defense policy. Civil-military cooperation is impossible to separate anymore and should be taken into account in state defense planning.**
- **Invest in cross-training and civilian participation in national exercises.**
- **Support trust-building between the security sector and civil society.**

2.5 REGULATION AND DIGITAL RESILIENCE

The Digital Services Act (DSA) offers a crucial regulatory foundation but requires robust national implementation. While Lithuania and Belgium have taken proactive steps, such as creating national AI and misinformation observatories, others lag due to limited staffing and unclear mandates.

Romania demonstrated the risk of under-regulation when TikTok was used to amplify foreign-backed messaging before elections. No moderation action was taken in time, and civic actors were left to fill the gap.

Czechia and Estonia emphasized the need for digital regulators to have investigative powers and the capacity to interface with both platforms and national security bodies. NGOs have stressed that transparency requirements must be enforced consistently across borders.

RECOMMENDATIONS:

- **Implement Digital Services Act with national oversight bodies that can audit platforms, issue binding decisions, and conduct investigations.**
- **Foster partnerships with civic tech and academic institutions to ensure oversight is data-driven.**

2.6 GRASSROOTS AND REGIONAL OUTREACH

Failing to involve regional and local actors weakens the state's communication impact. As multiple contributors emphasized, municipalities are the closest link to citizens, yet often remain underutilized. Initiatives such as the regional tours, senior digital literacy training, and informal pub events show that localized, face-to-face engagement works.

Municipalities, however, often lack strategic communication support. As the most trusted level of government, they should be equipped with adaptable toolkits, grants, and direct channels to national stratcom units.

RECOMMENDATIONS:

- **Embed communication resilience in regional development programs.**
- **Fund municipal outreach, intergenerational dialogue formats, and partnerships with libraries and cultural institutions, especially targeting vulnerable groups.**
- **Build a structural framework to involve municipalities in national communication strategies. Equip them with training, tools, and verified content.**
- **Prioritize building communities in time: Cooperate with CSOs and local actors to spark new collaborations. Building both formal and informal communities and trust amongst them in times of peace will go a long way when the crisis comes. Simply getting to know each other across institutions, sectors, and regions is what gets the "whole-of-society approach" from paper into reality. Sometimes, the best thing you can do is just to invite people for a beer.**

CONCLUSIONS

Hybrid threats are evolving in sophistication, but so too are our countermeasures. The Resilient Europe 2025 conference underscored that fragmented or short-term responses are insufficient. Resilience must be built into institutions, communities, and everyday communication. The path forward requires more than awareness. It demands coordination, investment, and moral clarity. European democracies have the tools; now they must summon the political will to act.

If there are lessons that emerge clearly from the discussions across panels and countries, they are these:

1. **We need data-driven communication.** Strategic communication must be grounded in audience research, behavioral data, and message testing. **We need to know what to say, how to say it, and to whom.** Without data, communication strategies risk being reactive, misaligned, or ineffective.
2. European leaders have to **take responsibility for framing defense against hybrid threats as a strategic priority** and accept that **strategic communication is a key pillar of building resilience** against them. However, verbal consensus on these issues is not enough. Any strategy can only be effective if institutions are capable of action, which requires clear mandate and resources, as well as legislation updated to correspond with current threats.
3. **We need grassroots activism and new actors.** National-level campaigns are necessary but insufficient. Change also comes from the ground up. New types of communicators - teachers, influencers, community leaders, librarians, veterans - must be empowered to reach different social segments, particularly those distrustful of traditional institutions.
4. **We need courage and the willingness to act.** Facing hybrid threats requires more than analysis. It requires decisive leadership, agile institutions, and legislative tools that reflect the complexity of today's risks. Institutional inertia and political caution must be overcome.

As one participant summarized:

> ***"We face a core challenge: people don't care. The role of strategic communication is precisely this: how do we make people care?"***

That is the ultimate test of democratic resilience, not just resisting the enemy, but reconnecting with our own societies.

It is only through responsive and actionable governance, inclusive dialogue, and sustained cooperation that Europe can build a democracy fit for the age of hybrid threats.

We may not have much time before the next big crisis hits - so we'd better start acting with courage now.

CENTER FOR
AN INFORMED
SOCIETY

www.informedsociety.cz