RESILIENT EUROPE:

BEST PRACTICES FROM ACROSS THE CONTINENT IN BUILDING RESILIENT SOCIETIES

AUTHORS

Veronika Víchová	CENTER FOR AN INFORMED SOCIETY
Nikoleta Nemečkayová	ASSOCIATION FOR INTERNATIONAL AFFAIRS
Jonáš Syrovátka	EUROPEUM INSTITUTE FOR EUROPEAN POLICY

CENTER FOR AN INFORMED SOCIETY

AMO.CZ

EUROPEUM
INSTITUT PRO EVROPSKOU POLITIKU
INSTITUTE FOR EUROPEAN POLICY

The Center for Informed Society (CIS) is a non-governmental, non-profit organization that is not affiliated with any political party. Our vision is a resilient and self-conscious democratic society that is not subject to authoritarian tendencies, defends human rights and the rule of law, and does not discriminate against anyone.

www.informedsociety.cz

Association for International Affairs (AMO) is a non-governmental not–for–profit Prague-based organization founded in 1997. Its main aim is to promote research and education in the field of international relations. AMO facilitates expression and realization of ideas, thoughts, and projects in order to increase education, mutual understanding, and tolerance among people.

www.amo.cz

EUROPEUM Institute for European Policy is a non-profit, non-partisan, and independent think-tank focusing on European integration and cohesion. EUROPEUM contributes to democracy, security, stability, freedom, and solidarity across Europe as well as to active engagement of the Czech Republic in the European Union. EUROPEUM undertakes original research, organizes public events and educational activities, and formulates new ideas and recommendations to improve European and Czech policy making.

www.europeum.org

This policy paper has been prepared with the support of Konrad Adenauer Stiftung.

www.kas.de

The views expressed in this publication are those of the authors and do not necessarily reflect the views of the donors and partners.

INTRODUCTION

In recent years, Europe has encountered a growing array of threats stemming from Russian malign influence, information interference, and hybrid warfare tactics that seek to destabilize democratic institutions, undermine public trust, and exploit societal vulnerabilities.

The **"Resilient Europe" conference** held in Prague in October 2024 gathered leading experts, policy-makers, and stakeholders from across Europe to share insights, best practices, and challenges faced in countering these threats.

This policy paper distills the core insights from the conference under three primary categories: hybrid threats, information manipulation in the digital space, and strategic communication. These categories encompass a broad range of actions taken by European nations and institutions to safeguard democratic resilience, and this paper further identifies the most pressing challenges and opportunities for future efforts.

1. HYBRID THREATS

Hybrid threats refer to actions conducted by state or non-state actors, whose goal is to undermine or harm a target by combining overt and covert military and non-military means.[1] While the state and its instantiations are primarily responsible for addressing these challenges, their multifaceted nature requires cooperation with multiple actors from civil society, private business or media. The concept of the whole-of-society approach encapsulates this approach to building resilience. This chapter provides examples of best practices in addressing hybrid threats and points out obstacles to implementing a whole-of-society approach.

Best practices

Framework for Cooperation

The whole-of-society approach requires an inclusive perspective on security and defense. A comprehensive approach applied in countries such as Estonia or Lithuania envisions cooperation between governmental, civilian, and NGO sectors to strengthen defense mechanisms. However, such cooperation requires a proper institutional framework that allows planning and coordination.

For example in Estonia, the **National Security and Defence Coordination Unit** at the Government Office of Estonia oversees management of national security and defence and has direct contact with the Prime Minister, while **the State Incident Situations Centre,** also under the Office of the Government, oversees situational awareness amongst both security institutions and the Government.[2] That way Estonia has an authorized coordination institution focused on both long-term planning and tactical exchange.

In the context of the European Union, such coordination should be not only horizontal but also vertical, bringing together EU-level institutions, national institutions, international NGOs and local civil society actors.

1 https://www.hybridcoe.fi/hybrid-threats/

2 For more information see the following link: https://www.researchgate.net/publication/384926859_Code_of_Resilience_Building_a_Functional_Ecosystem_for_Countering_FIMI_in_Estonia

Adaptable Legal and Regulatory Frameworks

The multifaceted, flexible and evolving nature of hybrid threats means that these activities – despite being malign – might be difficult to address due to gaps in legislation. Therefore, some countries such as Estonia, Czech Republic and others adopted a proactive approach and updated their legal frameworks to address specific tactics used by adversaries, including implementing their own national sanctions regimes, even though with varying levels of success in their implementation. Adapting legal frameworks in a timely manner provides a wider range of tools to counter hybrid threats.

Including general public

The whole-of-society approach is based on the assumption that every citizen will be able to contribute to the country's security. Therefore, the state has to invest in the preparation of citizens for crisis situations – including those related to hybrid threats – which in effect increases the resilience of the whole society.

Such efforts should start with increasing awareness about threats (e.g. disinformation and information operations) and introducing ways how to counter them on personal as well as community levels (e.g. media literacy). Examples of communication with the public can be brochure **If Crisis or War Comes issued by Swedish Civil Contingency Agency or "72 hours" preparedness concept promoted by Finnish authorities.**[3]

Challenges for the Future:

Political Fragmentation

The level of political commitment to counter hybrid threats varies among EU states which undermines a unified approach. The increase of populism and democratic backsliding further undermines the ability to cooperate and coordinate not only among states but also between state institutions and society. The short-term thinking of policy-makers related to the election cycle complicates the adoption and successful implantation of long-term strategies.

Coordination Shortfalls

Even if goodwill is present, coordination efforts might be undermined by a lack of time and resources. This is the case on multiple levels of Western-allied structures, for example between EU and NATO. Adversaries can exploit these gaps.

Adaptability of Hybrid Threats

Hybrid threats evolve as they adapt to technological developments and adjust to regional specificities to exploit existing societal problems. Since adversaries are constantly looking for new ways to undermine the resilience of Western states, the response has to be flexible and adaptable to their evolution.

3 For more information see the following links: (1) https://72tuntia.fi/en/?_ga=2.235574597.513345151.1634902063-440718003.1634902063 and (2) https://lastkaj.msb.se/Broschyren-Om-krisen-eller-kriget-kommer/brochure-sweden-english.pdf

2. INFORMATION MANIPULATION IN THE DIGITAL SPACE

As Europe stands at a pivotal moment with the Digital Services Act aiming to rein in social media giants and bring order to the digital chaos, a new challenge has emerged: the rise of AI. Combined with offline issues such as growing public frustration, uncertainty about the future, and an increasing preference for populist and far-right parties, this development further complicates efforts to tackle online manipulation. This chapter explores best practices from across Europe in countering manipulation in the digital space, while also addressing the emerging challenges ahead.

Best practices

Implementation of the Digital Services Act (DSA)

The implementation of the Digital Services Act (DSA) came at a crucial time of Meta suspending its CrowdTangle tool and X restricting its API access for researchers, offering new data streams and insights into social media governance. However, the DSA should not be seen as the sole solution to disinformation, as it primarily targets illegal and harmful content, not all forms of online manipulation.

To bridge this gap, **collaboration is needed not only between platforms and EU member states' Digital Services Coordinators (DSCs) but also between platforms and organizations like the Swedish Psychological Defence Agency.** These organizations play a critical role in managing content that falls outside the DSA's scope, including manipulative content that may not necessarily be illegal or harmful as well as disinformation that extends beyond the digital world, including TV, radio, newspapers, and social interactions with friends, families, and coworkers.

Entities like the Swedish Psychological Defence Agency are crucial for covering these areas, allowing for comprehensive research into the broader information environment enabling more effective policy development and testing.

Harnessing AI for Fact-Checking and Content Moderation

AI, like any technology, has dual potential: it can amplify issues like disinformation but also help combat them through enhancing mechanisms such as fact-checking and content moderation. Recognizing this, a **Czech media company, Seznam, has harnessed AI to manage discussions on their platform,** especially in politically sensitive contexts such as articles about Ukraine.

At the same time, Seznam remains vigilant about the biases AI may introduce and the potential for generating misleading outputs. To mitigate these risks, the company has crafted and enforced its own AI code for journalists, setting a precedent for ethical AI use in media. This strategy demonstrates that fighting disinformation with AI while maintaining credibility and ethical standards is feasible for even small companies, provided they make a concerted business decision to do so.

Cohesive Multinational Monitoring

Given the transnational nature of disinformation, the strategies to combat it should also be international. While several networks exist at the EU level, they are not always utilized effectively. However, these networks could significantly boost the efforts of individual national bodies and organizations fighting disinformation. For example, these national actors might encounter disinformation spreading within

their borders about another member state but lack the necessary country context or language skills needed to effectively counter it and clarify its inaccuracies.

A case in point is the pro-Russian narratives that circulated during Sweden's NATO accession. At that time, **Sweden informed its partners about the situation, helping them prepare for potential disinformation spreading to their countries.** Another benefit of this collaborative approach is that it prevents duplicity of effort – a narrative debunked by a fact-checking organization in one state can save efforts in another.

Using Humor to (Re)Build Public Trust

Using humor on social media can humanize state institutions and (re)build public trust. Humor is a familiar feature on these platforms. It highlights the human side of organizations and makes them more relatable. For example, strategic communication initiatives in the Czech Republic and by the

Slovak police have shown that humorous content not only grabs attention but also deepens understanding of the objectives behind disinformation campaigns without giving undue attention to the misleading narratives themselves. State institutions do not always have to create humorous content directly if it does not feel authentic. They can collaborate with influencers or even create an AI avatar to help produce this type of content. It is crucial that this content feels authentic and aligns with the identity of the institution to be effective.

Challenges for the Future:

Platform Accountability and Content Regulation

Although the Digital Services Act (DSA) marks progress in addressing online manipulation, it faces several challenges that affect its effectiveness. These include potential **data dumping, limited research capabilities, and reluctance to provide clear explanations of algorithms,** which hampers researchers' ability to interpret the data.

Additionally, there is an **insufficient number of content moderators** who are fluent in local EU languages, and the rise of AI-driven manipulation is not adequately covered by the Act. Another significant issue is the potential for audit capture, as platforms still control the data provided to independent auditors. Furthermore, the lack of similar regulations in the US, where many social media and AI companies are headquartered, complicates the global management of online content.

Technological Advances in Disinformation

Thus far, we have not seen the flood of AI-generated disinformation that was feared when the technology first emerged. However, this does not mean that AI has had no negative impact on the spread of disinformation, and the situation is likely to worsen in the years to come. Although not overwhelming, the number and quality of AI-generated content are on the rise.

Even if this content does not sway people towards a particular disinformation narrative, it still undermines their trust in the authenticity of online information and in whom they can trust. Likewise, it grants disinformers and populists a **'liar's dividend'—the ability to dismiss real evidence** of their missteps or political scandals as AI-generated and untrue, thus further blurring reality and complicating the work of fact-checkers and journalists.

Fragmented Response to Digital Manipulation

While Russia has successfully adapted its disinformation campaigns to target individual EU member states for years, it remains just one source of the issue and should be treated as such in the response from these states. Rather than maintaining fragmented and incompatible legislation in each state, a unified response is necessary to facilitate effective collaboration.

Currently, several obstacles hinder such a unified approach, including **varying perceptions of the threat level of disinformation** among local populations and political representatives, **different approaches to strategic communication** and information literacy, and the **politicization of combating foreign information manipulation**. With increasing frustration and uncertainty among EU populations and growing voter preferences for populist and far-right parties, these challenges are likely to worsen if not addressed.

Balancing Freedom of Speech and Regulation

Freedom of speech should not be mistaken for a right to spread falsehoods. Clear boundaries are necessary, yet defining them for harmful but legal content remains a challenge. Another layer of complexity arises from how **disinformers, along with populist and far-right politicians, exploit fears of free speech suppression.**

Recently, efforts to regulate social media and pass anti-disinformation laws have faced accusations of censorship and suppressing critical voices. These accusations have been leveraged to further fuel animosity towards the EU and certain national governments. This is not to say that regulation cannot be misused by individual governments for autocratic purposes. This is precisely why any effective regulation of the information space must include safeguards against such abuse and why the enforcement of these regulations should not be left solely to governments.

3. STRATEGIC COMMUNICATION

Strategic communication (StratCom) plays a vital role in fostering resilience within democracies, addressing hybrid threats, and countering disinformation across Europe. As discussed during the conference, effective state StratCom demands a comprehensive approach that includes transparency, local engagement, partnerships across sectors, and adaptable frameworks. This chapter highlights successful StratCom initiatives across Europe, while also examining ongoing challenges, using concrete examples from conference insights and recent practices across the EU.

Best Practices

Transparency and open communication

Transparency is foundational to effective StratCom. **Lithuania,** for instance, has prioritized an open communication culture across institutions, especially in the wake of Russia's invasion of Ukraine. Through structured communication strategies, the government has kept **citizens informed and prepared for potential threats, providing guidelines on emergency readiness and updates on national security.** This approach has strengthened public trust and bolstered Lithuania's societal resilience.

Another compelling example comes from the **UK's COVID-19 vaccine campaign.** During the pandemic, the UK government partnered with local leaders, religious figures, and community representatives to share accurate information about vaccines and counter misinformation about their safety. By using voices trusted in their communities, the government effectively addressed public concerns and encouraged vaccination uptake. This localized, transparent approach illustrates how StratCom can strengthen public confidence, even during a health crisis.

Localized messaging and trusted voices

In some contexts, localized messaging and engagement with trusted voices prove more effective than centralized approaches. In **Czechia,** for instance, authorities found that certain populations were disconnected from official messaging, prompting **efforts to reach these communities through trusted local representatives.** This approach allowed messages to resonate more deeply, fostering resilience against disinformation and promoting unity.

Sweden's Psychological Defense Agency also exemplifies this approach. The agency relies on **community voices during critical discussions, such as the debate on NATO accession,** amplifying the voices of community leaders to promote public support and counter misinformation. Sweden's emphasis on local, trusted voices in StratCom highlights the value of nuanced, community-based approaches for bolstering societal resilience.

Cross-sectoral partnerships

Multi-sector partnerships have been a cornerstone of effective StratCom. A prominent example is the **EU's European Democracy Action Plan,** which actively supports partnerships across sectors to address disinformation, safeguard election integrity, and foster media resilience. Under EDAP, initiatives like the European Digital Media Observatory bring together academic researchers, media organizations, and fact-checkers from across member states to combat disinformation and promote media literacy.

Additionally, the Nordic countries have pioneered partnerships that bridge government and civic sectors to build societal resilience. For example, **Finland's "Comprehensive Security" model** integrates government agencies, private sector partners, and local communities in regular preparedness exercises. These exercises simulate crisis scenarios, including hybrid threats, to build a coordinated response across sectors and ensure that communities are well-prepared.

Estonia's approach offers another model. The **Estonian government regularly collaborates with NGOs and local media, coordinating their efforts** to create a consistent message and reduce the influence of foreign disinformation. This whole-of-society strategy, which became more formalized after Russia's 2022 full-scale invasion of Ukraine, has strengthened societal cohesion and equipped citizens with tools to recognize and counter external influence.

Strategic frameworks for EU cohesion

The European External Action Service's (EEAS) StratCom division has become instrumental in exposing Russian-backed disinformation targeting the EU. The EEAS regularly published Disinformation Reviews, which centralize analysis of malign narratives and equip member states with insights to counter disinformation. This centralized approach encourages alignment across the EU, promoting a unified front against hybrid threats.

Challenges for the future

Sustaining public trust amid disinformation

One of the primary challenges facing StratCom efforts is sustaining public trust in democratic institutions amid widespread disinformation. For example, less than 25% of the Czech population currently expresses confidence in governmental institutions, highlighting a significant barrier to effective stratcom.

To address this, some countries have adopted a **"trust first" strategy** that prioritizes honesty and accountability, even when delivering challenging messages. Denmark, for instance, has tested transparent and straightforward communication on sensitive issues, aiming to earn public trust by avoiding overly positive spin. Yet sustaining trust requires **rethinking government messaging so it resonates with diverse audiences,** a challenge that demands ongoing attention.

Limitation of resources

It is not a coincidence that the countries listed in the previous "Best practices" section are the ones which **invest significant resources and employ hundreds of communication specialists.** Resource constraints remain a key issue for many other European nations. Countries like the Czech Republic and Slovakia, for instance, have faced limitations in funding and technical capacity for digital campaigns to counter disinformation. These constraints limit their ability to match larger countries' StratCom efforts. **EU support through collaborative funding or pooled resources** may offer a solution, helping smaller states build capacity and strengthen resilience.

Adaptability to evolving threats

Finally StratCom must remain flexible to fit the shifting and evolving digital technologies. The rising use of digital platforms and the interconnected change of communication preferences of the younger population will be another big challenge for more traditional communication channels of many state institutions.

CENTER FOR
AN INFORMED
SOCIETY

www.informedsociety.cz