Code of Conduct on Disinformation – Report of GLOBSEC for the period January – December 2025

Table of Content

Executive summary

Two main activities conducted by GLOBSEC's Centre for Democracy and Resilience ("the Centre") related to the Code are:

1. **Research and monitoring of disinformation:** The Centre regularly monitors trends in narratives and methods used to spread disinformation, with a particular focus on the Central and Eastern European region, Russian-linked information operations, and the integrity of electoral processes.

2. **Awareness raising on disinformation**: The Centre engages with the public, policymakers, journalists, and civil society through awareness-raising and capacity-building activities addressing disinformation, hybrid threats, and the integrity of the information space.

GLOBSEC participates in four subgroups of the Code's Permanent Task-Force: Crisis Response, Monitoring and Reporting, Generative AI, and the Working Group on Elections. GLOBSEC ensures consistent representation at Task-Force meetings and assigns dedicated staff to each subgroup.

Main activities during the monitoring period (January 2025 – December 2025):

GLOBSEC Trends 2025: Ready for a New Era?

Published on 14 May 2025, GLOBSEC Trends 2025 is the tenth edition of GLOBSEC's flagship annual survey covering public opinion across nine Central and Eastern European countries. The 2025 edition focused on security threat perceptions, democratic resilience, attitudes towards NATO and EU membership, and public vulnerabilities to hybrid threats including disinformation. Findings were presented at the GLOBSEC Forum 2025 and contributed to policy discussions with EU and national stakeholders.

Research on Foreign Information Manipulation and Interference (FIMI):

The Centre produced a series of research outputs investigating Russian-linked influence operations and disinformation infrastructure across Europe. Key publications included the Pravda Network investigation, investigations into Russian-linked influence operations targeting Moldova, and the Russia's Crime-Terror Nexus report (co-authored with ICCT) documenting the use of criminal networks as tools of hybrid warfare. These outputs received significant international media coverage, including in the Washington Post, Wyborcza, Business Insider Polska, TVP Info, and Ilta Sanomat.

Election integrity monitoring:

As part of the FIMI Defenders for Election Integrity (FDEI) project within the FIMI-ISAC framework, GLOBSEC actively monitored the information environments surrounding the 2025 Polish Presidential Election, 2025 Moldovan Parliamentary Election and the 2025 Czech Parliamentary Election. Monitoring resulted in the issuance of incident alerts, and the publication of comprehensive FIMI Response Team reports for all elections.

Media literacy and awareness-raising:

Throughout 2025, GLOBSEC participated in conferences, expert seminars, and public events across Europe, sharing insights on information manipulation during elections, hybrid threats, and information operations. Key speaking engagements included the NATO PDD conference in Brussels (January), events in Kosovo, North Macedonia, Berlin, Prague, the Chatham House event (November), or and the Cyber Security Nordic conference, fostering exchanges of know-how on FIMI trends and TTPs.

GLOBSEC along with other FIMI-ISAC partners supported civil society organisations in Poland, Czechia and Moldova, fostered exchange of know-how on observe and counter FIMI and hold or contributed to several workshops building their capabilities and skills to conduct investigations on FIMI.

III. Political Advertising	
Commitment 12 Relevant Signatories commit to increase oversight of political and issue advertising and constructively assist, as appropriate, in the creation, implementation and improvement of political or issue advertising policies and practices. [change wording if adapted]	
Measure 12.1	[insert wording if adapted]
Measure 12.2	[insert wording if adapted]
Measure 12.3	[insert wording if adapted]
QRE 12.1.1 (for measures 12.1-12.3) [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]

III. Political Advertising	
Commitment 13 Relevant Signatories agree to engage in ongoing monitoring and research to understand and respond to risks related to Disinformation in political or issue advertising. [change wording if adapted]	
Measure 13.1	
Measure 13.2	The scope of activities within Measure 13.2 only falls under the scope of countries, which will be included in GLOBSEC's research in the next years, depending on available projects and funding.
Measure 13.3	The assessment under measure 13.3 will be, so far, limited to Slovakia, as GLOBSEC has knowledge of the country's public administration, whereas it plans to expand to other countries in the future.
QRE 13.1.1 (for measures 13.1-13.3) [insert wording if adapted]	Outline relevant actions [suggested character limit: 2000 characters]

V. Empowering Users
Commitment 17

In light of the European Commission's initiatives in the area of media literacy, including the new Digital Education Action Plan, Relevant Signatories commit to continue and strengthen their efforts in the area of media literacy and critical thinking, also with the aim to include vulnerable groups. [change wording if adapted]	
Measure 17.1	[insert wording if adapted]
Measure 17.3	[insert wording if adapted]
QRE 17.3.1 [insert wording if adapted]	GLOBSEC is part of EDMO, BROD and CEDMO.

VI. Empowering the research community	
Commitment 29 Relevant Signatories commit to conduct research based on transparent methodology and ethical standards, as well as to share datasets, research findings and methodologies with relevant audiences. [change wording if adapted]	
Measure 29.1	• ***GLOBSEC Trends 2025: Ready for a New Era***?, published on 14 May 2025, provided a data-driven assessment of public opinion in nine CEE countries, offering critical insights into attitudes towards the EU, NATO, and key geopolitical and security issues. By employing a rigorous methodology and disseminating findings through public reports, expert briefings, and policy discussions, including at the GLOBSEC Forum 2025, GLOBSEC ensured that its insights were accessible to policymakers, researchers, and the broader public. This research played a vital role in informing evidence-based policymaking and enhancing understanding of regional dynamics. • GLOBSEC published the report ***Global Offensive: Mapping the Sources Behind the Pravda Network***. The investigation analysed over 4.2 million articles across 87+ subdomains, documenting how the Pravda Network functions as an AI-assisted propaganda infrastructure targeting audiences in the Visegrad Four countries and beyond. The report served as the basis for the A4E event "Behind the Curtain: Inside the Pravda Disinformation Network" (November 2025), co-organised by GLOBSEC and sponsored by the Polish Ministry of Foreign Affairs.

	• The report ***New Media Outlet Targeting Moldova Linked to Sanctioned Russian Network*** investigated the REST media outlet's connections to the sanctioned Russian threat actor Rybar, using metadata analysis, server timestamps, and shared technical infrastructure as evidence of coordination, contributing to the broader monitoring of Russian-linked influence operations in Eastern Europe. • The report ***Vocepentru Network***: A Russian-linked Influence Operation in Moldova, published ahead of the Moldovan parliamentary elections, exposed a network of fake polling websites mimicking pro-EU branding to manipulate public discourse and perceptions of electoral outcomes in Moldova.
QRE 29.3.1 [insert wording if adapted]	The research outputs and related methodologies of GLOBSEC during the monitoring period were published online.

VIII. Transparency Centre
Commitment 34 To ensure transparency and accountability around the implementation of this Code, Relevant Signatories commit to set up and maintain a publicly available common Transparency Centre website. [change wording if adapted]

VIII. Transparency Centre
Commitment 35 Signatories commit to ensure that the Transparency Centre contains all the relevant information related to the implementation of the Code's Commitments and Measures and that this information is presented in an easy-to-understand manner, per service, and is easily searchable. [change wording if adapted]

VIII. Transparency Centre

Commitment 36
Signatories commit to updating the relevant information contained in the Transparency Centre in a timely and complete manner. [change wording if adapted]

IX. Permanent Task-Force	
Commitment 37	
Signatories commit to participate in the permanent Task-force. The Task-force includes the Signatories of the Code and representatives from EDMO and ERGA. It is chaired by the European Commission, and includes representatives of the European External Action Service (EEAS). The Task-force can also invite relevant experts as observers to support its work. Decisions of the Task-force are made by consensus. [change wording if adapted]	
	GLOBSEC participated in the Permanent Task-Force throughout the monitoring period. GLOBSEC assigned specific staff members to each subgroup and ensured consistent representation at meetings, with cover arrangements in place when a primary representative was unavailable. Participation in the Working Group on Elections was particularly active in 2025 given GLOBSEC's extensive election monitoring work in Poland and Czechia.

X. Monitoring of Code	
Commitment 38	
The Signatories commit to dedicate adequate financial and human resources and put in place appropriate internal processes to ensure the implementation of their commitments under the Code. [change wording if adapted]	
Measure 38.1	
QRE 38.1.1 [insert wording if adapted]	GLOBSEC dedicated adequate financial and human resources to the implementation of its commitments under the Code during the monitoring period. The Centre maintained a dedicated team within the Centre for Democracy and Resilience responsible for Code-related activities, including monitoring, research, reporting, and Task-Force participation.

X. Monitoring of Code

Commitment 39

Signatories commit to provide to the European Commission, within 1 month after the end of the implementation period (6 months after this Code's signature) the baseline reports as set out in the Preamble. [change wording if adapted]

X. Monitoring of Code

Commitment 40

Signatories commit to provide regular reporting on Service Level Indicators (SLIs) and Qualitative Reporting Elements (QREs). The reports and data provided should allow for a thorough assessment of the extent of the implementation of the Code's Commitments and Measures by each Signatory, service and at Member State level. [change wording if adapted]

X. Monitoring of Code

Commitment 41

Signatories commit to work within the Task-force towards developing Structural Indicators, and publish a first set of them within 9 months from the signature of this Code; and to publish an initial measurement alongside their first full report. To achieve this goal, Signatories commit to support their implementation, including the testing and adapting of the initial set of Structural Indicators agreed in this Code. This, in order to assess the effectiveness of the Code in reducing the spread of online disinformation for each of the relevant Signatories, and for the entire online ecosystem in the EU and at Member State level. Signatories will collaborate with relevant actors in that regard, including ERGA and EDMO. [change wording if adapted]

X. Monitoring of Code

Commitment 42

Relevant Signatories commit to provide, in special situations like elections or crisis, upon request of the European Commission, proportionate and appropriate information and data, including ad-hoc specific reports and specific chapters within the regular monitoring, in accordance with the rapid response system established by the Taskforce. [change wording if adapted]

X. Monitoring of Code
Commitment 43 Relevant Signatories commit to provide, in special situations like elections or crisis, upon request of the European Commission, proportionate and appropriate information and data, including ad-hoc specific reports and specific chapters within the regular monitoring, in accordance with the rapid response system established by the Taskforce. [change wording if adapted]

X. Monitoring of Code
Commitment 44 Relevant Signatories commit to provide, in special situations like elections or crisis, upon request of the European Commission, proportionate and appropriate information and data, including ad-hoc specific reports and specific chapters within the regular monitoring, in accordance with the rapid response system established by the Taskforce.

Reporting on the signatory's response during an election

Executive summary

In 2025, GLOBSEC's Centre for Democracy and Resilience engaged in targeted election integrity activities across three elections: the 2025 Polish Presidential Elections (May 18 and June 1), the 2025 Moldovan Parliamentary Election (September 28) and the 2025 Czech Parliamentary Election (October 3–4) — as part of the FIMI Defenders for Election Integrity (FDEI) project under the FIMI-ISAC framework. As GLOBSEC co-authored severalreports on Polish Presidential Elections in May and July 2025, this submission covers only Moldovan and Czech Elections.

For both, GLOBSEC partnered with other organisations to conduct pre-election monitoring. GLOBSEC analysed online content across social platforms, websites, and Telegram channels, with a particular focus on foreign actors and their proxies. Asset mapping, identifying and documenting networks and TTPs used by foreign malign actors to spread election-related narratives, was a central component of this work. The two elections presented distinct threat profiles. In Czechia, no evidence of a large-scale foreign interference operation capable of influencing the election outcome was found; however, persistent structural FIMI infrastructure, including rebranded Russian state media successors, remained active throughout the monitoring period. In Moldova, FIMI reached unprecedented sophistication and scale, with coordinated influence operations — Storm-1516, Operation Overload, InfoLeaders, and REST Media — collectively generating an estimated 136.1 million views and 3.79 million interactions across 22 documented incidents.

Insights from monitoring contributed to the issuance of 15 incident alerts for the Czech election and 22 incident alerts for the Moldovan election. For For Moldova, FDEI members, for example, observed and reported FIMI cases targeting the Moldovan diaspora in EU member states.

Platform responsiveness varied significantly across both electoral contexts. While some VLOPs took swiftly down cotent and acocunts identified as part of a coordinated inauthentic network, other platforms were more reluctant In Moldova, while platforms removed more than a dozen inauthentic accounts linked to the InfoLeaders investigation, however, approximately 95 percent of content flagged by Moldovan national authorities was not acted upon.

In addition, 2025 elections in European countries showcased that platform's Ad Libraries, lacked sufficient transparency mechanisms, enabling opaque cross-border political advertising, while Telegram served as the primary command-and-control hub for Russian-linked operations with minimal moderation.

Research outputs from both monitoring periods were made publicly available. For Czechia, findings culminated in a comprehensive report on FIMI and elections co-authored with FDEI partners, and GLOBSEC co-authored to the Country Election Risk Assessment (CERA) published in September 2025. For Moldova, GLOBSEC contributed to providing situational awareness of FIMI, including two specific investigations — exposing REST Media's links to the sanctioned Rybar network (jointly with DFRLab) and uncovering the Vocepentru Network of fake survey websites — both of which contributed to the disruption of the documented operations. These outputs, together with the broader FIMI-ISAC's report on the Moldovan elections, provide evidence-based assessments of threats, actors, narratives, and platform responsiveness for both countries.

Reporting on the signatory's response during an election

2025 Czech Parliament Elections

Threats observed during the electoral period:

- **Deployment of Russian-linked proxy infrastructure:** Operation of rebranded Russian state media successors (neČT24/42tcen.com, Pravda Network, CZ24.news) to disseminate election-related disinformation narratives targeting party legitimacy and electoral integrity.
- **Coordinated Inauthentic Behaviour** (CIB): Detection of coordinated TikTok account clusters systematically promoting pro-Russian narratives and anti-establishment parties, with an estimated reach of 5–9 million views.
- **Electoral fraud meta-narratives:** Spread of the ''Romanian scenario'' narrative alleging that Czech elections would be manipulated by EU authorities or independent institutions, exploiting public uncertainty around the newly introduced postal vote.
- **Anti-RRS and censorship narratives:** Narratives portraying the RRS as a tool of censorship and foreign electoral manipulation, deployed by outlets with ties to Kremlin-linked infrastructure.
- **Cross-platform amplification cascades:** Narratives originating on Telegram and propagated across X/Twitter, Facebook, and TikTok, exploiting existing societal vulnerabilities around cost-of-living, defence spending, and Ukrainian refugees.
- **Deepfakes and AI-generated content:** Use of deepfake videos exploiting public figures for scam.

Empowering Users

Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.

Specific Action applied (with reference to the Code's relevant Commitment and Measure)	In reference to **Commitment 17**, Measures 17.1 and 17.3, GLOBSEC conducted the following user empowerment activities: • Provided situational awareness to platform representatives and relevant stakeholders on observed FIMI patterns and vulnerabilities in the Modlovan and Czech information environment during the electoral period. • Produced and contributed to reports, including the CERA and the post-election report, raising situational awareness of the Czech information space and FIMI threats ahead of and during the elections, publicly accessible to researchers, policymakers, and civil society. • Contributed to knowledge exchange within the FIMI-ISAC and FDEI consortium, and wider researcher community, including local researchers and CSOs, facilitating transfer of analytical insights, methodologies, and best practices across local organisations in Czechiaon the monitoring nformation space, analysis of FIMI, DISARM Framework or production of comparable incident reports.

	• Research findings were shared amongplatform representatives and otherstakeholders at the EU and national levels • Public reports contributed to broader societal situational awareness ahead of elections.
Empowering the Research Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	In reference to **Commitment 29**, Measure 29.1, GLOBSEC applied robust analytical methodology and ethical standards in monitoring the Czech electoral information environment. In cooperation with FIMI-ISAC/ FDEI partners GLOBSEC produced: • 15 FIMI incident alerts covering FIMI actors, TTPs operating in Czech information space and targeting the Czech parliamentary elections. • Co-authored CERA report for Czechia and final election report, documenting observed problematic narratives, FIMI and its TTPs. • Analytical findings were shared with Czech civil society partners, researchers, and the wider FIMI-ISAC community, strengthening, situational-awareness, cross-organisational analytical capacity and methodologies. • Collaboration within the FDEI consortium enabled systematic monitoring across borders and during various elections in 2025, with insights from the Czech case cross-referenced against parallel monitoring in other European information environments.
	• 15 documented incident alerts. • Public reports accessible to the research and policy communities, supporting sustained monitoring of foreign-linked operations in Central Europe. • Strengthened collaboration and cross-organisational analytical skills within the FIMI-ISAC/ FDEI consortium and local CSO/research community.

Reporting on the signatory's response during an election

2025 Moldova elections

Threats observed during the electoral period:

- **Operation Overload:** A large-scale Russian-linked content flooding operation generating thousands of repetitive, AI-assisted comments across Telegram and Facebook to create the illusion of mass dissent against Moldova's pro-European government and EU integration.
- **Storm-1516:** A Russian-affiliated information laundering campaign disseminating fabricated stories through a constellation of clone websites and mirrored domains. The operation collectively generated an estimated 59 million views, though a significant share of engagement was inauthentic.
- **InfoLeaders — paid influencer network:** A paid network of at least 253 social media accounts coordinating inauthentic activity across TikTok, Facebook, and Instagram, generating more than 55 million views across 28,000 pieces of content. Accounts were paid through Russian financial intermediaries linked to fugitive oligarch Ilan Shor and the sanctioned Promsvyazbank.
- **REST Media — Russian proxy outlet:** A new website established by actors linked to the sanctioned Kremlin-affiliated Rybar network, targeting Moldovan and EU audiences with anti-EU and anti-government narratives. REST's TikTok content generated over 3 million views; its articles were amplified by the Pravda Network across Europe.
- **Vocepentru Network — fake civic surveys:** A coordinated network of fake survey websites mimicking pro-EU branding to manipulate public opinion, collect user data through tracking pixels linked to Russian-affiliated infrastructure, and portray the ruling party as unpopular.
- **Fabricated diaspora observer recruitment:** A Facebook ad campaign (HumanGo) paying Moldovan diaspora citizens across Europe up to €30,000 to report fabricated election "irregularities," reaching over 1 million users across the EU and UK, linked to the EU-sanctioned Stark Industries Solutions.
- **Anti-EU, anti-government, and security meta-narratives:** Sustained amplification of narratives portraying EU integration as a sovereignty threat, framing Moldova's government as corrupt and subservient to Western interests, and exploiting war anxiety, religious divisions, and economic hardship to depress confidence in democratic institutions.
- **Hate speech and antisemitic content:** AI-generated antisemitic videos targeting EU leaders and President Maia Sandu, viewed nearly 300,000 times across TikTok, X, and Instagram, combining conspiracy imagery with electoral disinformation.

Empowering Users

Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.

Specific Action applied (with reference to the Code's relevant Commitment and Measure)	**In reference to Commitment 17,** Measures 17.1 and 17.3, GLOBSEC conducted the following activities in the context of the 2025 Moldovan elections: • Provided monitoring of information space and situational awareness with relevant stakeholders on observed FIMI patterns and vulnerabilities in the Moldovan information environment prior and during the electoral period.

	• Published investigative outputs (REST Media and Vocepentru reports) that were disseminated publicly, contributing thus to broader societal awareness of active FIMI operations targeting Moldovan voters and Moldovan diaspora in the EU countries. • Presented findings and experiences from monitoring elections in Moldova, Poland, and Czechia at the ODIHR Seminar on election monitoring and other expert roundtables including a Chatham House's event (November 2025), contributing to knowledge-sharing with the European research and policy community.
	• Findings shared with European research and policy communities.
Empowering the Research Community	
Outline approaches pertinent to this chapter, highlighting similarities/commonalities and differences with regular enforcement.	
Specific Action applied (with reference to the Code's relevant Commitment and Measure)	**In reference to Commitment 29,** Measure 29.1, GLOBSEC applied robust analytical methodology and ethical standards in monitoring the Moldovan electoral information environment. Research outputs: • Contributed to the production of FIMI incident alerts covering FIMI operations targeting the 2025 Moldovan parliamentary elections. • Published the *New Media Outlet Targeting Moldova Linked to Sanctioned Russian Network* report (joint investigation with DFRLab), exposing REST Media's links to the Rybar network using metadata forensics, server analysis, and infrastructure attribution. • Published the Vocepentru Network: A Russian-linked Influence Operation in Moldova report, exposing a network of fake survey websites linked to Russian-affiliated infrastructure and designed to manipulate Moldovan public opinion ahead of the elections. • Analytical findings were shared with Moldovan civil society partners, researchers, and the wider FIMI-ISAC/ FDEI consortium, strengthening cross-organisational analytical capacity and collaborative monitoring methodologies. • Collaboration within the FDEI consortium enabled structured information-sharing between Moldovan and European partners, providing Moldovan actors with indirect access to EU-level coordination and monitoring tools.
	• 22 incident alerts provided situational awareness on FIMI operatins and used TTPs • Public reports produced by FIMI-ISAC members provided understanding of FIMI operations in Moldova. • REST Media domain became unavailable within days of the public investigation of the investigation. • Vocepentru Network's amplification infrastructure was disrupted following the public exposure. • Strengthened cross-organisational collaboration and analytical methodologies within the FIMI-ISAC/ FDEI consortium and local researchers/CSOs.