Submission by Human Constanta on external oversight and accountability of anti-extremism and counter-terrorism measures in Belarus

24 February 2026

hr-ct@odihr.pl

In response to the OSCE Office for Democratic Institutions and Human Rights (ODIHR) call for submissions on the oversight of human rights compliance in state measures to prevent and counter terrorism, Human Constanta provides the following input. This submission focuses on documented practices in Belarus concerning counter-extremism and counter-terrorism legislation and enforcement, highlighting systemic gaps in transparency, independent oversight, and accountability, and their implications for the protection and effective enjoyment of human rights.

Human Constanta's engagement in oversight of counter-terrorism measures

Human Constanta is a Belarusian human rights organisation focused on the promotion of public interests and joint actions in response to modern challenges in the field of human rights. The organisation's key areas of work include monitoring the practices in the fields of anti-extremism laws and policies, digital rights, migrants' rights, and anti-discrimination. One of Human Constanta's core areas of work is monitoring legislation and state policies on combating "extremism" and "terrorism" in Belarus and their impact on the human rights situation. Expert materials produced by Human Constanta are referenced by international mandates – for instance, the UN Special Rapporteur on the situation of human rights in Belarus and the OSCE Moscow Mechanism.

In our quarterly reviews of the application of anti-extremism and counter-terrorism legislation in Belarus in the context of human rights, we examine legislative acts, publications by state media, pro-government Telegram channels, independent media, and human rights organizations, as well as various lists and catalogues maintained by government agencies related to "extremism." We also occasionally receive information directly from victims of the arbitrary application of these laws.

While Human Constanta meaningfully contributes to independent monitoring and public accountability through open-source analysis and documentation, our work is carried out in a highly restrictive environment. Access to relevant and reliable information on the application of counter-terrorism and anti-extremism measures in Belarus is increasingly limited, and there are no formal avenues for civil society participation or consultation with state oversight bodies. Key challenges affecting our monitoring work include, *inter alia:*

- restricted access to court decision databases and court hearing schedules on the Supreme Court's website;
- limited access to official government resources from outside Belarus;
- the concealment or non-publication of disaggregated official judicial statistics related to "extremist" and "terrorist" offences;
- ongoing persecution of human rights organisations and individuals cooperating with them, including the designation of resources as "extremist materials" or "extremist formations", and the detention and prosecution of volunteers;
- a noticeable decline in publicly available information from pro-government sources, including a reduction in the publication of videos and other materials related to detentions.

These constraints significantly undermine transparency and accountability in the application of counter-terrorism measures and necessitate greater reliance on open-source intelligence, and indirect documentation methods.

Identified gaps and challenges in the external oversight of counter-terrorism measures in Belarus

In Belarus, "anti-extremism" legislation has become a central tool for silencing dissent and controlling civic and political life. A defining characteristic of Belarusian legislation is the extremely broad and inconsistent definition of "extremism," which varies across different normative acts. Since "terrorist activity" is explicitly incorporated within the legal definition of "extremism", counter-terrorism measures in Belarus are effectively implemented as a component of the wider anti-extremism framework.

Provisions relating to "extremism" and "terrorism" are embedded across multiple legal instruments, including the Laws "On Countering Extremism" and "On Combating Terrorism," relevant articles of the Criminal Code and the Code of Administrative Offenses, the Law "On Citizenship" (which allows for the deprivation of citizenship for "extremism-related offenses"). Specialized government-maintained lists track "extremist" materials, organizations, formations, and individuals, as well as registers of individuals and organisations related to "terrorist activities." These laws are systematically applied to restrict both online and offline speech, targeting democratic activists, independent journalists, human rights defenders, and administrators of social media channels. Extra-judicial practices, such as labeling political prisoners as "prone to extremism" in detention, further extend the repressive reach of the state.

As defined in the Law "On Combating Extremism" and the Law "On Combating Terrorism," the responsibility for combating "extremism" and "terrorism" lies solely with state authorities. These

include law enforcement, state security, prosecution, border and customs services, the Investigative Committee, the Presidential Security Service, the Ministry of Defense, and other government agencies in culture, education, media, religion, and science. No civil society actors, independent experts, or external oversight mechanisms are formally included in the system of anti-extremism enforcement.

This exclusive concentration of authority in government institutions effectively excludes any independent scrutiny, participatory oversight, or external accountability, leaving counter-extremism policy entirely under the control of the executive and security apparatus.

Opaque management of official "extremist" and "terrorist" lists in Belarus

Belarus maintains a range of formal mechanisms aimed at combating extremism and terrorism, each operating under tightly controlled and opaque procedures.

The official Republican list of extremist materials serves as one of the central instruments of the country's anti-extremism framework. Materials are added to this list following evaluations conducted by the Republican Commission for the Assessment of Symbols, Attributes, and Informational Products, which is tasked with identifying signs of "extremism." The commission is composed entirely of state officials, security personnel, deputies, and academics from state universities, without independent experts. Its conclusions are generally formulaic and form the primary basis for including publications on the official list. Courts typically formalize these decisions in closed proceedings with extremely limited participation by affected parties. Decisions are often effectively predetermined, with prosecutors requesting that inspected materials be added to the list even before a court ruling, leaving content owners with no real opportunity to defend themselves. This structure illustrates a highly centralized, opaque system that excludes civil society and independent scrutiny.

The similar approach applies to the List of organizations, formations, and individual entrepreneurs involved in "extremist" activities. Groups of citizens are designated as "extremist formations" based on decisions of the Ministry of Internal Affairs (MIA) or the State Security Committee (KGB), made extrajudicially. The texts of these decisions are not published, making it impossible to review the reasoning behind them. The Law "On combating extremism" does not provide any procedure for removal of formations from the list, which would likely require overturning the original MIA or KGB decision – access to which is effectively impossible.

Moreover, Belarusian citizens are included in the List of individuals involved in "terrorist" activities en masse, based on decisions of the KGB, which can rely not only on court convictions but also on

mere accusations. The reasoning behind these decisions is not disclosed, often referring to vaguely defined criminal provisions, and the process is entirely opaque, offering individuals virtually no meaningful avenue to contest their inclusion.

In Belarus, website blocking is one of the measures used in the state's anti-extremism and counter-terrorism policy. Access to dozens of platforms, including independent media outlets, civil society resources, and opposition initiatives, is routinely restricted following the identification of "extremist content" on these sites. However, the official List of restricted access identifiers of Internet resources to which access is restricted is non-public, with access limited to state authorities, Internet service providers, and a small number of designated entities. While it is technically possible to check the status of individual websites via the official portal of the State Inspectorate for Communications of the Ministry of Communications and Informatization of Belarus (BelGIE), there is no public access to the full list of blocked resources. The criteria for inclusion are opaque, notifications to resource owners are often delayed or absent, and there is no formal mechanism for independent verification or challenge. Reasons for blocking are rarely explained in detail, typically limited to brief, vague references to the responsible authority, offering no meaningful insight into the justification or legal basis for the restriction.

Across all these mechanisms, decisions are made by state authorities through opaque procedures, with limited transparency, minimal opportunity for affected parties to challenge their inclusion, and little to no independent or judicial oversight.

Lack of oversight in Belarusian "extremism" and "terrorism" cases

The handling of "extremism" and "terrorism" cases in Belarus is characterized by secrecy and restricted access to information. Nearly all criminal cases related to "extremism" and "terrorism" in Belarus are conducted behind closed doors. Official communications from state authorities provide only fragmentary information, often citing vague legal provisions, leaving the specifics of most cases opaque. Transparency is further restricted by limited public access to court decision databases and court hearing schedules on the Supreme Court's website, as well as by the designation of journalistic and human rights defending resources as "extremist materials" or "extremist formations," and the detention or prosecution of independent observers. Independent scrutiny is essentially absent: in cases involving online speech, such as alleged "incitement of enmity," independent assessments or expert evaluations of the content are almost never taken into account.

This combination of closed hearings, restricted access to information, and repression of monitoring actors effectively excludes meaningful external oversight, preventing individuals, civil

society, or international observers from assessing the lawfulness or proportionality of the measures applied.

Belarus' participation in the Shanghai Cooperation Organisation

On 4 July 2024, Belarus completed its accession as a full member of the Shanghai Cooperation Organisation. As a result, it became fully bound by the legal framework of the Shanghai Convention on Combating Terrorism, Separatism and Extremism and related SCO instruments. The Convention contains broadly formulated definitions of "terrorism", "separatism" and "extremism" and establishes co-operation on the basis of mutual recognition of such acts by member states. It further provides that nothing in the Convention prejudices the application of other international treaties or national legislation that may allow for a broader interpretation of these terms. This formulation permits reliance on expansive domestic definitions in cross-border co-operation. The mutual recognition framework, combined with the possibility of broader domestic definitions, may facilitate cross-border enforcement measures (including information exchange, designation, and co-operation in criminal matters) without sufficient alignment with international human rights standards, notably the principles of legality, foreseeability and proportionality

Operational co-ordination in the SCO is carried out through the Regional Anti-Terrorist Structure (RATS), which reportedly operates under conditions of near-total confidentiality. RATS maintains a database of individuals and organisations designated by member states as "terrorist", "extremist" or "separatist", facilitating their cross-border identification and co-operation among security agencies. However, the criteria for inclusion in this database, the evidentiary standards applied, and the procedures for challenging or removing a designation are not publicly accessible. There is no independent external oversight or appeal mechanism at the SCO level. In the absence of effective national scrutiny over executive engagement in this framework, this creates a structural accountability gap.

Belarus' participation in the SCO counter-terrorism architecture introduces an additional layer of international cooperation that is largely shielded from transparent review, raising systemic concerns regarding external oversight and human rights safeguards.

Surveillance and digital control in Belarus' counter-extremism and counter-terrorism framework

The Belarusian authorities rely on technologies of surveillance as tools of suppressing dissent, masquerading as "anti-extremism" and "counter-terrorism" measures. Whether through routine

monitoring of public social media accounts, hacking into private devices, video monitoring, or excessive data collection, – surveillance is essential for Belarusian digital autocracy.

Although the exact methods of surveillance of citizens by Belarusian authorities and the algorithms underpinning them are not public, some comments from state officials confirm the use of surveillance and shed some light onto the tools used. For instance, Investigative Committee officials mentioned that "it is hard to imagine a criminal case, in which the investigators would not look into the information on the phone connections of the suspect." He also mentioned a special automated information system "Footprint," used since summer 2021 as a tool monitoring the digital footprint of suspects.

Another notorious tool used by the Belarrusian authorities to track dissidents is the "Kipod" facial recognition software developed by "24x7 Panoptes" company. The latter is a subsidiary of Synesis – a notorious Belarusian software developer, included in the European Union, United Kingdom and the United States sanctions lists for providing authorities with the video surveillance platform and aiding therewith the state in repressing the civil society and democratic opposition. Synesis also became the target of restrictive measures introduced by the United Kingdom and the United States. The algorithm became integrated into the Republican Public Safety Monitoring System after winning the tender for the selection of the technical operator for this national system. One of the events, reportedly proving the platform's application for political persecution, is the arrest of Mikalai Dziadok – a prominent political activist and blogger. The security forces set up surveillance on Dziadok's acquaintance and managed to track down his regular routes by seizing video recordings from the Minsk metro surveillance cameras, embedded into Kipod platform. Belarusian media outlet Balsat dubbed the software "Lukashenko's digital eyes."

On 18 October 2022, Alexander Lukashenko issued Decree № 368 on the interaction of telecommunication operators, telecommunication service providers and owners of Internet resources with law enforcement and secret services. The Decree institutionalizes surveillance and takes it to an unprecedented level. In addition to existing surveillance practices, the Decree forces online resources, such as email providers, messengers, online retailers, taxi and car sharing services, to retain data about the users and provide the authorities with direct remote access to such data. It means that now law enforcement and secret services can obtain and correlate telecom data with online service data. These powers are not limited by any reasonable safeguards and cannot be challenged in courts due to their covert nature and factual impossibility to provide for the fair trial in Belarusian courts.

Belarus' anti-extremism and counter-terrorism framework combines broadly defined legal powers, centralized state control, opaque procedures, and pervasive digital surveillance, creating an environment where judicial review, independent oversight, and civil society participation are

effectively excluded. The integration of domestic measures with international mechanisms under the SCO further exacerbates the risks of cross-border enforcement without sufficient alignment with international human rights standards. In practice, these structures and technologies enable the authorities to suppress dissent, restrict freedoms of expression and association, and exercise near-total control over both online and offline civic space, raising systemic accountability gaps and significant risks for the protection of human rights.

Recommendations for strengthening oversight and accountability in counter-terrorism measures

Belarus' experience demonstrates that broadly defined anti-extremism and counter-terrorism laws, centralized state control, opaque procedures, and pervasive surveillance significantly limit independent oversight and undermine human rights. To address these challenges, OSCE participating States should consider measures at multiple levels of governance to strengthen external scrutiny, ensure compliance with human rights standards, and improve accountability.

1. *Amend overly broad anti-extremism legislation and prevent politicized implementation.* States should review and amend counter-extremism and counter-terrorism legislation to ensure that definitions of "extremism," "terrorism," and related offences comply with the principles of legality, legal certainty, necessity, and proportionality under international human rights law. Vague and expansive provisions that enable arbitrary or politically motivated application should be repealed or narrowed to prevent misuse against dissenting voices, independent media, and civil society actors. Where legislative provisions remain in force, their implementation must not be politicized. Enforcement practices should be guided by objective, transparent criteria and subject to effective judicial oversight, ensuring that counter-terrorism measures are not used to suppress legitimate exercise of the rights to freedom of expression, association, peaceful assembly, and political participation.

2. *Ensure transparency and access to information.* State actors, including law enforcement and intelligence agencies, should implement transparent procedures for designation, listing, and enforcement of counter-terrorism measures. Criteria, evidentiary standards, and processes for removal or challenge of designations must be publicly available. Publication of court decisions, access to hearing schedules, and summaries of enforcement actions are essential for external scrutiny. Transparency should extend to the use of surveillance technologies, including automated systems, digital monitoring platforms, and facial recognition tools, with clear explanations of legal bases and safeguards for the protection of privacy and due process.

3. *Strengthen judicial review and remedies.* States should ensure that individuals and organizations subject to counter-terrorism measures have access to effective legal remedies. Independent courts should be able to review executive decisions, examine evidence, and provide timely recourse to contest inclusion in lists or restrictions on speech, movement, or property.

4. *Establish independent oversight mechanisms.* States should create or empower independent oversight bodies with specific mandates to monitor counter-terrorism and anti-extremism measures. These bodies should have authority to review designations of individuals and organizations, assess enforcement practices, and issue binding recommendations or orders. Oversight institutions must be structurally independent from executive agencies, security services, and prosecutorial authorities, with legal guarantees protecting their autonomy. Sufficient staffing, expertise in human rights law, and technical knowledge of surveillance and digital monitoring systems are critical to enable meaningful review.

5. *Integrate international and cross-border oversight standards.* States should align domestic counter-terrorism measures with international human rights obligations and ensure that participation in regional frameworks does not undermine transparency or accountability. International cooperation agreements must include provisions for oversight, information sharing under human rights safeguards, and review of cross-border enforcement actions. Oversight bodies should have the capacity to examine international cooperation, joint operations, and data exchanges to assess compliance with legal and ethical standards.

6. *Promote civil society participation.* External oversight should systematically include civil society organizations, independent media, human rights defenders, which are currently persecuted en masse. Governments should establish structured mechanisms for consultation, enabling meaningful engagement in monitoring, reporting, and policy development. Participation must be protected from any form of retaliation, intimidation, or legal consequences, ensuring that civil society actors can contribute freely. Access to information and participation should be secured in ways that allow independent verification and enhance accountability.