

## **Digital Transnational Repression: A Growing Threat to Civic Space. An example of Belarus**

***Remarks at the OSCE Supplementary Human Dimension Conference “Safeguarding Civic Space in the Digital Age”. Session 1, “Digital threats to civic space”***

***Vienna, 11 May 2026***

**by Yuri Dzhibladze, Head of Human Rights and Rule of Law Unit, International Strategic Action Network for Security – iSANS**

I am speaking on behalf of International Strategic Action Network for Security, an analytical and advocacy centre working to detect and counter hybrid threats to democracy, rule of law and sovereignty of states.

In the era when civic space is under massive attack, authoritarian regimes do not limit themselves to repression within their national borders. They reach globally to suppress the voices and activities of their critics outside their territorial jurisdiction, thus making even democratic countries unsafe for exiled dissenters. In recent years, targets of transnational repression (TNR) have broadened from traditional dissidents – such as human rights defenders, journalists, and political opposition – to include academics, lawyers, diaspora communities, and supporters of victims. TNR is manifested through various tactics, aimed at silencing and punishing exiled opponents and intimidating dissenters inside the country. As thousands of pro-democracy figures have had to flee their countries of origin in the last few years due to escalating repression, we are witnessing the increase in TNR by a number of states in the OSCE region.

Rapid development of digital technologies has facilitated the increase and transformation of TNR practices. Artificial intelligence (AI) has further transformed the TNR landscape and exponentially amplified TNR’s reach and impact. AI-powered content moderation tools make it easier for regimes to control the narrative and suppress opposition without the need for costly human intervention.

My remarks are based on analysis of digital TNR employed by the Lukashenka regime. Already in 2023, Belarus was considered to be among the top ten states practising TNR. However, none of the other states has had recently taken up TNR with as much intensity as the regime in Belarus. The regime’s TNR practices are not unique; they are used by authoritarian states all over the world. Our research conducted last year shows that there is a clear symmetry and cooperation in TNR practices between Belarus and Russia. Our report “Transnational Repression in Belarus: A Brutal Tool of the Persecution of Dissent by the Lukashenka Regime”, presented by iSANS at the Warsaw Human Dimension Conference last October, has been used as a background material by UN experts and members of the European Parliament in addressing the issue.

The main tools of digital TNR can be categorised into the following groups:

- 1) the use of spyware to engage in unauthorised surveillance of a target’s computer or mobile phone;
- 2) the hacking of social media, email, and other internet accounts to acquire information about the activities and networks of targeted persons and launch their criminal persecution on this basis;
- 3) the abuse of social media to engage in sustained and coordinated campaigns of disinformation and intimidation, including with the assistance of newly emerging artificial intelligence tools;
- 4) the acquisition of location data and the use of face recognition technology to track the target’s movements; and
- 5) the use of DDoS attacks to take down websites that with critical information.

All of these tools have been used by the Lukashenka regime to target Belarusian exiles in various countries. Examples include the following:

Between August 2020 and January 2023, several Belarusian independent journalists and opposition activists based in Europe were targeted with Pegasus spyware. In addition, in December 2025 it became known that the Belarusian KGB uses a previously unknown espionage software for surveillance. The program, which was named Resident Bat after its discovery and investigation by *Reporters Without Borders*, allows access to call logs, microphone recordings, SMS messages, messages from encrypted messengers, and local files. It is disguised as a regular application.

Lukashenka's special services regularly hack websites, social network accounts, chats, private chatbots, and messenger accounts of independent media, civil society, and political opposition to gather information on individuals and organisations in exile, including evidence that is used in criminal proceedings against them conducted *in absentia*. Targets included *BYSOL* solidarity initiative and *Dissidentby* documentation project. Such activities not only discourage participation in civic initiatives but also enable their discrediting, potentially leading to their closure. In the biggest case, a chatbot of the *Belarusian Hajun Project*, a prominent open-source intelligence monitoring initiative created to track military activity on Belarusian territory, was hacked by the regime's secret services in February 2025. This led to the arrests of approximately 200 people inside Belarus who had sent monitoring information to the project. They were charged with "facilitation of extremist activities", and many were sentenced to prison terms.

In a different type of activity, the regime's agents create fraudulent chatbots of solidarity initiatives and monitoring projects to lure people there, identify and persecute them.

Security officers harass the exiles in social networks and threaten them with abduction and forcible return to Belarus as well as persecution of their relatives inside the country. These messages serve to instil in the exiles a sense of the regime's constant attention, undermine their psychological state, destroy trust in those around them, and force emigrants into cooperation with secret services.

Further, the Lukashenka regime monitors public activities of the Belarusian diaspora by hiring individuals to film participants of peaceful protests against the regime in various countries. Digital technologies allow to quickly transfer the recordings to the customer and use face recognition tools. As a result, the Investigative Committee of Belarus reported that it had identified hundreds of participants of demonstrations in Poland, Lithuania, Czech Republic, and other countries, and opened criminal investigation against them. This is a clear attack on freedom of peaceful assembly and freedom of expression.

Finally, severe DDoS attacks on independent online resources have targeted lately *Nasha Niva* media, *Reform.news*, the *Belarusian Investigative Centre*, Sviatlana Tsikhanouskaya's Office, and many others.

Victims of digital TNR explained that it generated concerns about their privacy and created feelings of insecurity, fear, uncertainty, distress, and burnout. Victims also expressed concerns regarding the safety of their families and community. Others reported that digital TNR pushed them to adopt different patterns of behaviour, such as keeping a low profile online, posting pictures of specific locations only after leaving them, and asking that conference participants' biographies be kept offline. They also commented that digital TNR impacted how they socialise and interact with others. In particular, they restricted communications with people in their home country and avoided socialising in the host country. Self-censorship can also lead victims to avoid speaking to law enforcement in the host country about threats to personal safety. The mere possibility of being subjected to digital TNR pushes activists towards self-

censorship. Digital threats also deter the wider diaspora. It is particularly disturbing because of the role they play in transnational advocacy efforts and fighting human rights abuses in their home countries.

As with other TNR instances, cases of digital TNR are typically considered human rights violations, infringing on the rights to privacy and freedom of expression, among others. However, they also distort public debate, impede the host state's adherence to fundamental norms of international law, and undermine the host state's sovereignty and capacity to successfully integrate immigrants.

On the basis of our research, we suggest the following recommendations to democratic states and OSCE institutions with regard to combating TNR, including digital TNR:

To OSCE bodies:

1. Put the issue of TNR high on the agenda and treat it as a multi-dimensional problem and a specific threat to both human rights and sovereignty of states;
2. Develop recommendations or guidelines on combating TNR;
3. Develop comprehensive global and regional strategies for tackling TNR, grounded in a consolidated approach combining the goals of protecting human rights of the targets of repression and safeguarding state sovereignty;
4. Take into consideration systematic TNR practices by states when considering their involvement and initiatives in international bodies.

To participating States:

5. Establish specialised bodies with the mandate to:
  - monitor manifestations of TNR at a regional and national level,
  - strongly react to specific cases,
  - conduct investigation,
  - provide protection,
  - develop recommendations or guidelines on combating, preventing, and eradicating TNR,
  - develop relevant documents to acknowledge the TNR nature of certain actions by states and include country-specific guarantees and protections against TNR;
6. Invoke the Moscow Mechanism in respect of states actively using TNR and digital TNR, such as Belarus and Russia.