European Liberal Forum

POLICY PAPER
No 36 | February 2026

A New Age of Espionage and Intimidation

Countering Digital Transnational Repression in the EU

Abstract

Espionage tactics are evolving, with spy software offering cheaper alternatives to physical undercover agents. Authoritarian regimes increasingly rely on information and communications technologies to monitor, intimidate, and silence dissidents beyond their borders. This phenomenon, known as digital transnational repression (DTR), presents a growing threat to liberal democracies. DTR violates individual liberties, threatens state sovereignty, and undermines the liberal international order. The EU's current response remains fragmented and reactive, lacking a dedicated policy framework, a proactive deterrence, and punitive mechanisms. This paper proposes a comprehensive EU strategy, one that introduces a distinct DTR policy, uses strategic intelligence for deterrence, and establishes punitive measures for enabling states and private actors. Adopting such measures would strengthen the EU's internal sovereignty, protect human rights, and reinforce liberal democratic norms in the face of rising global authoritarianism.

Marie Inasaridze
Eurasian geopolitics expert,
MA in Global Security & Strategy

Extraterritorial authoritarianism in the EU

On January 2021, activist Carine Kanimba, a dual US-Belgian citizen of Rwandan descent, discovered that she had been the victim of an intensive surveillance campaign. A forensic analysis revealed that Kanimba's phone had been infected with Pegasus spyware, a powerful commercial surveillance tool that grants the operator complete access to the target's personal device. The analysis revealed that the spyware was likely active during the activist's meetings with high-level EU officials, including the Belgian Minister of Foreign Affairs.

> While the proliferation of ICTs has empowered digital activism, it has also reduced the costs and risks of extraterritorial political control.

Kanimba's case is not an isolated incident, as authoritarian regimes increasingly rely on information and communications technologies (ICTs) for repressive efforts. Between 2020 and 2023, the digital rights organisation Access Now documented eight cases in Europe in which exiled journalists were targeted with Pegasus-enhanced surveillance.[1] These cases shed light on the underreported phenomenon of digital transnational repression (DTR) – illiberal regimes' reliance on digital tools to suppress dissent outside their national borders. While the proliferation of ICTs has empowered digital activism, it has also reduced the costs and risks of extraterritorial political control . Authoritarian regimes employ DTR to silence dissent, thus undermining democratic principles and the liberal international order.

The EU's current approach to combating DTR remains fragmented and reactive, lacking a clear definition, a dedicated policy framework, and proactive deterrent mechanisms. As the EU struggles to address this growing issue, its strategic rivals continue to consolidate power and undermine liberal values globally. As ICTs become the primary tool for obstructing democratic and liberal processes, actively combating DTR becomes more crucial than ever. Addressing this issue

[1] Access Now (2024), 'Exiled, Then Spied On: Civil Society in Latvia, Lithuania, and Poland Targeted with Pegasus Spyware', Access Now, 30 May, https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.

is of strategic importance, as DTR violates state sovereignty and interferes with state self-interests.

The EU has recently introduced the European Democracy Shield and the Strategy for Civil Society initiatives, carried out by DG CONNECT and DG JUST. Through these initiatives, the EU can implement a proactive, systemic approach to DTR by considering the following recommendations: (1) distinguishing DTR from other hybrid threats, (2) using strategic intelligence for deterrence, and (3) instating punitive measures against enabling state actors and private companies.

The new face of repression

Transnational repression is 'a set of physical and digital tactics used by governments to stifle dissent among political exiles or diaspora communities.[2] While the physical manifestations of transnational repression receive substantial coverage, the digital aspects have only recently gained traction, with ICTs playing a central role in enhancing authoritarian governments' repression tactics. Such infringements of privacy, intimidation, and silencing grossly violate individual liberties, while the subsequent sovereignty concerns undermine the rules-based international order. In an increasingly hostile geopolitical world, actively defending core liberal principles becomes vital for effectively challenging rising global authoritarianism.

Diasporas serve as key members of transnational advocacy networks, as they employ ICTs to encourage resistance at home and expose regime atrocities to international audiences. These mass communications provide a 'digital scaffolding' that can fuel liberal social change.[3] However, the same digital environment facilitates state surveillance, intelligence hacking, and intimidation.[4] Authoritarian leaders rely on repression to stay in power, while ICTs threaten state monopoly over information and fuel oppositional mobilisation. Therefore, regimes that are highly intolerant of dissent view cyberspace as an arena requiring policing.[5]

ICTs empower authoritarian actors to pursue intimidation by offering inexpensive alternatives to traditional repression methods. Rather than sending agents abroad to spy on and intimidate critics, they increasingly rely on basic forms of hacking,

[2] Freedom House (2025), 'NEW DATA: Mass Incidents Mark Dramatic Year of Transnational Repression, as 23 Governments Silence Exiles', 6 February, https://freedomhouse.org/article/new-data-mass-incidents-mark-dramatic-year-transnational-repression-23-governments-silence.

[3] D. M. Moss (2018), 'The Ties That Bind: Internet Communication Technologies, Networked Authoritarianism, and "Voice" in the Syrian Diaspora', *Globalizations*, 15(2), 265–282, https://doi.org/10.1080/14747731.2016.1263079.

[4] A. Dukalskis, S. Furstenberg, Y. Gorokhovskaia, J. Heathershaw, E. Lemon, & N. Schenkkan (2022), 'Transnational Repression: Data Advances, Comparisons, and Challenges', *Political Research Exchange*, 4(1), 2104651, https://doi.org/10.1080/2474736X.2022.2104651.

[5] Moss, 'The Ties That Bind'.

such as phishing campaigns or distributed denial-of-service (DoS) attacks. These attacks are harmful in multiple ways: on top of impairing access to information, breaching the victim's security, and limiting their ability to engage in free speech[6], hacking attacks can bring substantial financial losses and reputational damage to activists.[7]

Furthermore, a successful hacking attack against a single activist can expose a whole network of associate dissidents within and outside state territory.[8] Diaspora communities often enforce self-censorship and silence out of fear for themselves and their families. The self-censorship is exacerbated by the host states' failure to provide the victims with the appropriate resources to combat these threats and uphold their fundamental human rights. Through DTR techniques, authoritarian states challenge the EU's ability to guarantee the safety and rights of political exiles or, as in Kanimba's case, even those of European citizens. These tactics threaten the EU's ability to maintain domestic authority, protect individual liberties, and uphold the rules-based international order.

By violating the rights of their citizens abroad, authoritarian states also obscure the role and interests of the host state. DTR can violate state sovereignty and interfere with states' self-interests by distorting public discourse and weakening government institutions, the rule of law, and social cohesion.[9] Thus DTR must be framed as an internal security concern, rather than as a mere threat to 'foreigners'. Kanimba's case highlights an even bleaker reality – by violating the privacy of one citizen, perpetrators can indirectly breach the security of high-level officials internationally. This tactic thus presents a direct threat not only to the liberal order but also to state officials, as any citizen who is in contact with government officials can become a tool for foreign infiltration.

The EU acknowledges foreign interference as a threat to European security and the rule of law. However, transnational repression has not been securitised, meaning that the EU has not presented (D)TR as a significant security threat.[10]

---

6 N. Aljizawi & S. Anstis (2022), 'The Effects of Digital Transnational Repression and the Responsibility of Host States', *Lawfare*, https://www.lawfaremedia.org/article/effects-digital-transnational-repression-and-responsibility-host-states.

7 P. V. Falade (2023), 'Decoding the Threat Landscape: ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks', *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(5), https://doi.org/10.32628/CSEIT2390533.

8 M. Michaelsen & J. Thumfart (2023), 'Drawing a Line: Digital Transnational Repression Against Political Exiles and Host State Sovereignty', *European Journal of International Security*, 8(2), 151–171, https://doi.org/10.1017/eis.2022.27.

9 Ibid.

10 S. Furstenberg (2025), 'The European Union's Response to Transnational Repression: Are We Moving Towards Securitisation?' *European Journal of International Security*, 1–25, https://doi.org/10.1017/eis.2025.2.

The EU's reactive democracy

The current EU approach to digital transnational repression is ineffective mainly due to the absence of a clear definition, an established policy framework, and proactive preventive measures. The much-anticipated Democracy Shield fails to even mention transnational repression, reinforcing the perception that this tactic is separate from pressing threats to European democratic resilience.[11] The EU Strategy for Civil Society, although more solution-driven, outlines only reactive, protective measures for victims of transnational repression.[12] The strategy highlights EU initiatives such as ProtectDefenders.eu and the Human Rights Defenders Mechanism, which are valuable for providing emergency support to human rights defenders (HRDs) in third countries. However, these mechanisms provide emergency assistance only to HRDs outside the EU, leaving exiled activists vulnerable to repression within EU territory. Furthermore, the strategy remains fundamentally reactive, offering no proactive or systemic measures, and continues to concentrate on the physical manifestations of transnational repression, omitting solutions to its digital forms.

As of now, transnational repression in itself is not a defined policy area, and the existing policy documents make no effort to distinguish it from other forms of hybrid threats. The EU's 'whole of society' approach in countering cyber operations and other hybrid threats largely ignores state-sponsored transnational attacks against individual civil society actors.[13] Currently, the EU relies on fragmented mechanisms to address challenges caused by (D)TR, such as providing emergency funds to human rights defenders, bureaucratic assistance with visa requests, and sanctions against perpetrators. However, these fragmented applications of response mechanisms address separate instances post-factum; the EU lacks a systemic, preventive capacity to tackle the issue, especially within cyberspace. Addressing digital aspects of TR is also crucial for the physical protection of its targets, as the majority of physical violations against exiles are preceded or accompanied by some form of digital threat.[14] Therefore, such a fragmented, reactive approach does not provide the appropriate means to prevent transnational repression, either in physical or in digital terms.

---

11 European Commission (2025), *Communication on the European Democracy Shield*, 12 November. https://commission.europa.eu/document/2539eb53-9485-4199-bfdc-97166893ff45_en.

12 European Commission (2025), *Communication on the EU Strategy for Civil Society, 12 November*, https://commission.europa.eu/document/8c30975d-bc1c-4415-8dcd-a71cb28f3662_en.

13 Michaelsen & Thumfart, 'Drawing a Line'.

14 Ibid.

Policy recommendations

The EU needs a proactive approach to digital transnational repression, with a dedicated policy, a preventive system, and punitive mechanisms. DTR must be distinguished from other hybrid threats, as these operations target specific individuals rather than manipulating the informational environment via massive censorship and disinformation campaigns. Regulating cyberspace is essential for tackling DTR, as the proliferation of ICTs drastically reduces the costs and risks associated with extraterritorial political control. This allows the EU's strategic rivals to silence dissidents, who are instrumental in challenging repressive regimes, thus ultimately consolidating authoritarian power and undermining liberal values. The EU needs to shape the normative environment, implement preventive measures, and punish perpetrators .

> The EU needs to shape the normative environment, implement preventive measures, and punish perpetrators.

Shaping the normative environment

The first step towards effective policymaking is to have a distinct policy. As discussed above, the EU currently does not have a dedicated framework for addressing transnational repression, let alone DTR. It is crucial to distinguish (D)TR from the general hybrid-threat umbrella, provide a clear definition of the concept, and build an effective policy that proactively tackles these threats. A standardised common understanding of the concept is crucial for moulding Member States' interpretation of the phenomenon and tackling the issue systemically. The policy must include both physical and digital aspects of transnational repression, as perpetrators often penetrate the two dimensions simultaneously. A standardised definition must then be followed by a two-pillar defence system, leveraging strategic intelligence for proactive deterrence and punitive mechanisms.

Strategic intelligence as a preventive tool

Strategic intelligence is essential for addressing complex challenges such as DTR, particularly when authoritarian regimes employ various repressive mechanisms to consolidate power. Intelligence is vital for enhancing our understanding of the scope and evolution of DTR, as it helps identify the actors, methods, and digital infrastructures involved. This includes tracing the origins of cyber intrusions, mapping networks of proxies and intermediaries, and assessing the strategic intent behind coercive digital campaigns. However, governments are often reluctant to disclose evidence obtained through intelligence operations. Coordination between intelligence analysts and policymakers is especially crucial in a rapidly evolving cyberspace , where adaptive techniques and emerging challenges, such as AI-powered cyberattacks and malware,[15] necessitate interdisciplinary solutions for effective prevention and deterrence. To enhance the EU's ability to detect and attribute DTR activities, deeper horizontal and vertical cooperation is required, including closer partnerships with academics, cyber experts, civil society, and DTR victims, as well as greater intelligence-sharing across EU and national intelligence services.

> Coordination between intelligence analysts and policymakers is especially crucial in a rapidly evolving cyberspace.

Personal experiences from victims of DTR serve as an additional source of valuable strategic intelligence. Those who have previously faced digital transnational repression can provide first-hand insight into early warning signs, recurrent repressive tactics, and effective mitigation practices. Active and continuous engagement with vulnerable HRDs and previous targets is essential for developing a proactive EU strategy. Systematic communication with competent authorities would convert these insights into practical preventive tools, which can also be integrated into guidance for newly arrived exiles. Such cooperation establishes a strong knowledge-sharing network, improving the detection of early warning signs and reinforcing confidence in EU support mechanisms.

Punishing perpetrators and enablers

Beyond deterrence purposes, intelligence is also crucial for punishing perpetrators. The EU must consider expanding law enforcement powers to criminalise and prosecute acts of transnational repression. Considering the overlaps with

[15] Falade, 'Decoding the Threat Landscape'.

espionage operations, EU law enforcement and counterintelligence agencies, such as Europol, Eurojust, and ENISA, can play a key role in detecting and constraining the activities of perpetrators, and bringing them to accountability. The approaches used in the FBI's criminal cases[16] and Sweden's criminalisation of 'refugee espionage[17] provide examples of systemic prosecutions of DTR.

Furthermore, states and private companies enabling digital transnational repression must also be held accountable. In an alarming number of documented DTR cases, perpetrators used Pegasus spyware, which was developed by the Israeli cyber-arms company NSO Group. Since the software is categorised as a defence technology, the Israeli defence ministry must approve the sale of Pegasus licenses to foreign governments. Yet despite the deliberate misuse of this terrorism-detection software, the ministry continues to authorise sales of these products to countries with a long history of severe human rights violations.[18] Due to these violations, the US Department of Commerce blacklisted the NSO Group back in 2021.[19] The EU must follow suit in treating these violations as threats to national security and must punish enablers, be it through diplomatic pressure on state actors or sanctions on private companies. Additionally, the EU must pressure the Israeli government to ensure that the sale of defence technology is in line with basic liberal values.

Moving forward

The European Democracy Shield introduces an important deliverable in the form of the European Centre for Democratic Resilience, which provides valuable infrastructure for moulding new DTR policies. The centre can host a dedicated working group responsible for developing this framework, while DG CONNECT and DG JUST offer higher-level guidance to ensure alignment with broader EU priorities. When taking these necessarily first steps, the EU must be wary of subsequent challenges, such as attributing digital attacks to their perpetrators, uneven cooperation among Member States, active cooperation with the targets of DTR, and the development of secure and interoperable databases. Tackling DTR offers the EU an opportunity to address growing threats to liberal and democratic processes by protecting basic human rights, strengthening internal sovereignty, and bolstering cross-national cooperation. Breakthroughs in these areas have immense potential for promoting liberal values and deepening European integration.

16 Furstenberg, 'The European Union's Response'.

17 Freedom House (2022), *Sweden: Transnational Repression Host Country Case Study,* https://freedomhouse.org/report/transnational-repression/sweden.

18 D. E. Sanger, N. Perlroth, A. Swanson, & R. Bergman (2021), 'U.S. Blacklists Maker of Pegasus Spyware, NSO Group', *New York Times,* 3 November, https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html.

19 M. Pollet (2021), 'NGOs Urge EU to Sanction Israeli NSO Group', Euractiv, 3 December, https://www.euractiv.com/short_news/ngos-urge-eu-to-sanction-israeli-nso-group/.

References

Access Now (2024). 'Exiled, Then Spied On: Civil Society in Latvia, Lithuania, and Poland Targeted with Pegasus Spyware'. Access Now, 30 May. https://www.accessnow.org/publication/civil-society-in-exile-pegasus/.

Aljizawi, N., & Anstis, S. (2022). 'The Effects of Digital Transnational Repression and the Responsibility of Host States'. *Lawfare*. https://www.lawfaremedia.org/article/effects-digital-transnational-repression-and-responsibility-host-states.

Dukalskis, A., Furstenberg, S., Gorokhovskaia, Y., Heathershaw, J., Lemon, E., & Schenkkan, N. (2022). 'Transnational Repression: Data Advances, Comparisons, and Challenges'. *Political Research Exchange*, 4(1), 2104651. https://doi.org/10.1080/2474736X.2022.2104651.

European Commission (2025). *Communication on the European Democracy Shield*, 12 November. https://commission.europa.eu/document/2539eb53-9485-4199-bfdc-97166893ff45_en.

European Commission (2025). *Communication on the EU Strategy for Civil Society*, 12 November. https://commission.europa.eu/document/8c30975d-bc1c-4415-8dcd-a71cb28f3662_en.

Falade, P. V. (2023). 'Decoding the Threat Landscape: ChatGPT, FraudGPT, and WormGPT in Social Engineering Attacks'. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(5). https://doi.org/10.32628/CSEIT2390533.

Freedom House (2022). *Sweden: Transnational Repression Host Country Case Study*. https://freedomhouse.org/report/transnational-repression/sweden.

Freedom House (2025). 'NEW DATA: Mass Incidents Mark Dramatic Year of Transnational Repression, as 23 Governments Silence Exiles', 6 February. https://freedomhouse.org/article/new-data-mass-incidents-mark-dramatic-year-transnational-repression-23-governments-silence.

Furstenberg, S. (2025). 'The European Union's Response to Transnational Repression: Are We Moving Towards Securitisation?' *European Journal of International Security*, 1–25. https://doi.org/10.1017/eis.2025.2.

Michaelsen, M., & Thumfart, J. (2023). 'Drawing a Line: Digital Transnational Repression Against Political Exiles and Host State Sovereignty'. *European Journal of International Security,* 8(2), 151–171. https://doi.org/10.1017/eis.2022.27.

Moss, D. M. (2018). 'The Ties That Bind: Internet Communication Technologies, Networked Authoritarianism, and "Voice" in the Syrian Diaspora'. *Globalizations*, 15(2), 265–282. https://doi.org/10.1080/14747731.2016.1263079.

Pollet, M. (2021). 'NGOs Urge EU to Sanction Israeli NSO Group'. Euractiv, 3 December. https://www.euractiv.com/short_news/ngos-urge-eu-to-sanction-israeli-nso-group/.

Sanger, D. E., Perlroth, N., Swanson, A., & Bergman, R. (2021). 'U.S. Blacklists Maker of Pegasus Spyware, NSO Group'. *New York Times*, 3 November. https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html.

About ELF

The European Liberal Forum (ELF) is the official political foundation of the European Liberal Party, the ALDE Party. Together with 56 member organisations, we work all over Europe to bring new ideas into the political debate, to provide a platform for discussion, and to empower citizens to make their voices heard. Our work is guided by liberal ideals and a belief in the principle of freedom. We stand for a future-oriented Europe that offers opportunities for every citizen. ELF is engaged on all political levels, from the local to the European. We bring together a diverse network of national foundations, think tanks and other experts. In this role, our forum serves as a space for an open and informed exchange of views between a wide range of different EU stakeholders.

A liberal future in a united Europe

liberalforum.eu

/europeanliberalforum
/europeanliberalforum
@eurliberalforum
eurliberalforum
@eurliberalforum.bsky.social

DOI: 10.53121/ELFPP36

ISSN: 2736-58165

Graphic Design: Altais
Cover image: FREEPICK

This publication received financial support from the European Liberal Forum.