'Fighting back against transnational repression'

Hearing of the Legal Affairs & Human Rights Committee of the Parliamentary Assembly of the Council of Europe, 13 May 2025

Written observations of Alex Tinsley, Expert

Any views expressed in this document are my own, not those of Doughty Street Chambers, any association(s) I am affiliated with, or any client. For any materials I have cited, summarised or paraphrased, see the original.

Introduction

1. This document is the basis for my oral comments before the Legal Affairs & Human Rights Committee ('**the Committee**') of the Parliamentary Assembly of the Council of Europe ('**PACE**') on 13 May 2025.

2. The Committee has invited me to speak in the context of its ongoing file '***Fighting back against transnational repression***', of which it seized itself by motion of 25 June 2024.[1] I am grateful for the invitation.

3. I am a barrister at Doughty Street Chambers in London. I am a member of the international working group Lawyers Against Transnational Repression ('**LATR**'). I am part of the task force of the European Criminal Bar Association ('**ECBA**') leading on contribution to the ongoing INTERPOL reform process. I also act as Senior Legal Consultant for the non-governmental organisation Fair Trials ('**Fair Trials**'); I drafted their Fair Trials' first major output on INTERPOL in 2013. I was previously heard by the Committee on the topic INTERPOL in May 2015 in Yerevan.

4. Ten years on from my last intervention here, states continue to author transnational repression ('**TNR**'). But the tactics are bolder, more pervasive, and more advanced, aided by technology. And there are signs that efforts may be made to row back some of the progress already achieved. It is timely that the Committee is revisiting the issue, following its various reports on this topic in recent years.

5. My observations will comment on the following topics:

[1] Doc. 16017 - Motion for a resolution - Working document.

a. INTERPOL – The current reform initiative pursued by INTERPOL and the need for European states to participate constructively in this; and long-standing issues still requiring reform.

b. Mutual legal assistance ('**MLA**') – The need for individual safeguards and monitoring generally; the current topic of MLA provisions in new cybercrime treaties; and the question of Article 18 ECHR liability of Council of Europe states for cooperating with TNR.

c. TNR more generally – On the issue of defining TNR; the need for holistic policy covering national security and human rights aspects of TNR; the topic of TNR targeted at lawyers; and the role of the Platform to Protect Journalists in the TNR context.

INTERPOL

General background

Risk of abuse: need for safeguards

6. I will not rehearse background matters which will already be familiar to this Committee. In short, states do seek to abuse the system (in particular red notices), using it as an instrument of TNR.

7. The issue is not new, but remains as current as ever. I need only refer to the very recent 'China Targets' investigation of the International Consortium of Investigative Journalists, detailing how Beijing '*abuses international institutions, including Interpol […] to terrorize its critics and extend its repressive tactics worldwide*'.[2]

8. Which places the focus on the controls within INTERPOL's General Secretariat ('**IPSG**') (more specifically the Notices and Diffusions Task Force ('**NDTF**')) and the remedies available to individuals via the Commission for the Control of INTERPOL's Files ('**CCF**').

9. PACE has played an important role over time both in sounding the alarm as to risks of abuse of INTERPOL and supporting the organisation by providing constructive and principled support to its reform processes.[3] We are now in the next instalment of that dialogue.

---

[2] ICIJ, *About the China Targets investigation*, 28 April 2025 (link).

[3] See Resolution 2161 (2017) *Abusive recourse to the Interpol system: the need for more stringent legal safeguards*; and Resolution 2315 (2019) *Interpol reform and extradition proceedings building trust by fighting abuse*.

The CCF and INTERPOL's judicial immunity

10. It is important to remember why the CCF matters so much in this discussion. First, it is the main route for individuals to seek remedies. Secondly, it operates as an internal system of justice, the effectiveness of which is critical to INTERPOL's judicial immunity. This Committee acknowledged in 2017 that the CCF's must have sufficient powers and offer sufficient procedural guarantees if that immunity is to be justified.[4]

11. This is why the Committee needs to pay very careful attention to any failure to strengthen the CCF's procedures as it then recommended, and even more so to any changes which risk *weakening* the CCF's powers.

Work of the Committee on the Processing of Data

The CPD in general: transparency needed

12. In 2019, the Working Group on the Processing of Information ('**GTI**') was converted to a standing committee of the General Assembly called the Committee on the Processing of Data ('**CPD**')[5] which would review INTERPOL's rules on a continuing basis.

13. The founding resolution stipulated that the CPD would meet once per year; delegated to the CPD itself '*the power to* ***adopts its own terms of reference*** *… taking into account proposals by member countries* […]'; and requested the CPD to '***report on its work*** *to the General Assembly at its annual sessions*'. The resolution also '[invited] ***INTERPOL's members to participate in and contribute to*** *the work of the* [CPD]'.

14. I would point out that **(a)** the CPD's self-defined terms of reference are not public; **(b)** the CPD's annual reports have not to date been public; and **(c)** INTERPOL has not disclosed who participates in the CPD.

15. I know of no public data on the latter point. I find it relevant to point out that in 2023, the INTERPOL General Assembly passed a resolution[6] which '*TASKS the* [CPD] *to consider the proposals regarding the settlement of disputes, improving the quality of assessment of INTERPOL notices and diffusions and supervision measures for data processing, submitted by* ***Belarus*** (…) *and to report back to the General Assembly* (…) *for further*

---

[4] See Resolution 2161 (2017) *Abusive recourse to the Interpol system: the need for more stringent legal safeguards*, §§6 and 8.2.

[5] Resolution No 3 of the 2019 (Santiago) General Assembly GA-2019-88-RES-03 (download).

[6] Resolution No 9, 91st Session (2023 – Vienna) GA-2023-91-RES-09 (download).

discussion and approval'. In 2025, **Belarus** publicly advertised its involvement in the CPD,[7] disclosing that there were 70 participants from 45 countries. This indicates that Belarus has recently contributed to and is currently participating in the CPD's work. Let me point out that Belarus attracted condemnation in 2024 for obtaining the arrest of a journalist in Serbia in breach of INTERPOL rules.[8] Belarus is said to have the third-highest number of imprisoned journalists of any country.[9]

16. In 2025, INTERPOL published the first of what appears to be several consultations inviting civil society to contribute to the CPD's work.

17. The webpage[10] states that the CPD had '*recently launched a process to review the legal framework governing the work of the CCF*', inviting civil society input on two specific issues only (discussed below). It is not clear how (e.g. upon whose proposal) the CPD defined the current topics.

18. The page states that '*calls for contributions on other topics related to the work of the CCF* […]*, including new topics that may be proposed by civil society, will be launched in the future*' (my emphasis). This suggests that the CPD is focused on CCF reform. To my knowledge, INTERPOL / the CPD has not sought external input as to possible other topics, whether as to the CCF or with regard to INTERPOL more generally.

19. Having regard to the above, I suggest:

    a. The Committee should **seek information from INTERPOL and/or call for transparency** as to (a) **the CPD's current terms of reference;** (b) the **make-up of current CPD participation;** and (c) **any report submitted by the CPD to the General Assembly in 2025** – in due time to enable effective public scrutiny.

    b. The Committee should **Encourage Council of Europe Member States to participate actively and constructively in the CPD**. This would ensure representation of Council of Europe states and

---

[7] 'Belarus attends meeting of Interpol Committee on Processing of Data in Lyon', *BelTA*, 18.03.2025 (link).

[8] Committee to Protect Journalists, *Belarus's dangerous push for Serbia to extradite journalist Andrey Gnyot*, 17 September 2024 (link). INTERPOL deleted the notice which led to his arrest, but he was detained for a year pending extradition: see Balkan Insight, *Belarus Activist Freed From Detention in Serbia Leaves for EU*, 1 November 2024 (link).

[9] Reporters Without Borders, 2023 Round-Up – Journalists detained, held hostage and missing (link).

[10] Review of CCF Statute – Call for Contributions (accessed 07.05.2025) (link).

ensure that Council of Europe priorities – such as the protection of journalists – are taken into account in these discussions.

c. The Committee should **seek clarity from INTERPOL as to the schedule of CPD consultations**, including when civil society will have the opportunity to propose new topics, both about the CCF and about INTERPOL more generally, as this timeline is likely to overlap with the Committee's work on this file.

<u>The CPD's current topic: delaying CCF involvement</u>

20. The two topics identified in the recent call for civil society input to the CPD process are: '*(1) the procedure for the examination of new requests and (2) the right to access, correct and delete data – misuse of CCF proceedings*'. I reproduce the revisions as proposed by the CPD as **Appendix I** in case the webpage disappears. I focus on the first point.

21. Broadly, these proposed changes seek to circumscribe the CCF's role so that it can only begin considering an individual request – and can only issue any decision on provisional measures in relation to it – after IPSG has reached a '*final compliance decision*' on the state's notice request. The reforms require the CCF to forward information it receives to IPSG to take into account in that '*compliance review*'. The thrust is to re-centre primary decision-making at IPSG level, with the CCF acting as a review body thereafter. This affects so-called pre-emptive requests, where the person seeks to prevent publication of an abusive notice ab initio. Currently the CCF seems to be involved from the outset; under these reforms, its action would be delayed until after IPSG reached its decision.

22. The ECBA task force on INTERPOL responded to this consultation. I will supply our contribution to the Committee. LATR also contributed.[11] Among the ECBA's points, I would emphasise these (my summary):

a. **The CPD's proposed reform is unconstitutional** – Under the INTERPOL Constitution, the CCF's role is to ensure compliance with INTERPOL's rules in the processing of information. Such processing occurs as from the moment a request is received, and CCF competence arises as from that point. Reforms to the CCF Statute cannot, and should not seek to, constrain that role more narrowly.

[11] LATR, *[LATR] responds to the call for contributions of the [CPD] […]*, 6 April 2025 (link). I did not participate in (or therefore sign) the specific LATR contribution, being focused on the ECBA contribution. Having considered the LATR contribution, I broadly agree with it.

While the objective of sequencing the decisions of IPSG (executive decision-maker) and CCF (review body) is not inherently objectionable, this should be achieved compatibly with the terms of the Constitution. The CCF Statute should therefore recognise that the CCF retains the power to intervene in a case in parallel to IPSG review where necessary, e.g. in an urgent medical case.

b. **The CPD's proposed reform could be read as undermining CCF provisional measures and the rule of law** – On one reading, the reforms permit INTERPOL to find a notice request compliant *and then immediately publish the requested notice* before the CCF can begin to act, in particular by issuing any provisional measures decision. That would run contrary to the very purpose of provisional measures, which is to preserve the status quo and avoid irreversible harm pending a final decision. However, we say that '*compliance decision*' (the reaching of a legal view as to compliance) and '*publication*' (the formal act of publishing the notice) are clearly not one and the same thing, and that IPSG must pause before undertaking the latter to ensure that the CCF has an opportunity to issue provisional measures. We suggested a corresponding amendment to Article 74 RPD to spell out that obligation.

c. **The sharing of an individual's information with IPSG** (which would seem to become mandatory under the CPD's proposals) is a concern. As IPSG has seconded staff, and as the NDTF engages with member countries, applicants have a real concern that their private data will be shared. Special protections provided by the CCF Statute are not replicated in the CPD's reforms. This is likely to create a lot more complication and, unhelpfully, increase CCF workload.

23. I emphasise the critical importance of the second issue. This Committee has previously emphasised the critical importance of interim measures to the efficacy of the CCF, a key parameter for INTERPOL's immunity.

24. Having regard to the above, I suggest –

a. The Committee should **encourage the INTERPOL to respect the CCF's constitutional role**, and in particular to **ensure the CCF has the power to issue effective provisional measures.**

b. The Committee should **encourage INTERPOL to explain how NDTF practice will protect confidentiality** (see also below).

Areas actually requiring reform

25. Together with ECBA colleagues we have been considering key issues for reform, which will shortly be reduced to a formal policy paper. I will supply it to the Committee when it is published. For now, I set out below preliminary indication of our core topics, with my point of view:

    a. **CCF delays** – Delays are still a problem, with deadlines exceeded. There should be greater engagement to update applicants and explain delays; ore resources are required; and changes to the case management process might assist.

    b. **CCF Disclosure (equality of arms)** – Eight years on from the entry into force of Article 35 of the CCF Statute, the process has not (contrary to the Committee's hope in 2017[12]) become "*fully adversarial*", a key measure of its credentials as an alternative system of justice. Applicants still do not have any sight of what the NCB is arguing until it appears in the final decision. This paradoxically leads to applicants applying to reopen CCF cases based on what they learn from a decision, undermining finality and creating significant further delay. We will propose a workable practical model providing for an open exchange while accommodating confidentiality issues.

    c. **CCF Revision** – Currently, applicants apply to reopen CCF decisions based on information discovered in the CCF's decision, because it is not disclosed beforehand. This is clearly not how the system should operate. Ensuring equality of arms in CCF proceedings would remove the need for this. Moreover, issues with delays are acute in relation to revision. It is also unclear whether revision is required where an NCB issues a new notice request after a first refusal.

    d. **CCF Appeal** – CCF decisions remain debatable qualitatively. INTERPOL should commission a feasibility study for the establishment of an appeal body so that applicants could challenge specific decisions, while still allocating resources effectively.

    e. **Diffusions** – There appears to be no mechanism for diffusions to be reviewed by the NDTF prior to circulation. Thus a diffusion may still be issued by an NCB, only for the police cooperation request to be found contrary to INTERPOL's rules / any related red notice request

[12] See the report of Bernd Fabritius (Doc. 14277) accompanying resolution 2161 (2017).

to be refused. By which time, the data are already circulated. A technological solution enabling prior review seems to be elusive.

f. **Recognition of extradition decisions** – The ECBA's existing work recognises a distinction between permanent and non-permanent grounds for refusal of extradition. Logically, INTERPOL should update antiquated resolutions on extradition to ensure that where extradition is refused on universal grounds, this should presumptively lead to the deletion of a notice, unless (the burden being shifted to it) a state can establish that something has changed and that it can properly claim to be able to obtain extradition.

g. **Asylum / refugee policy** – There is a need for further clarity on the application of INTERPOL's refugee policy, in particular for those who may be refugees but whose application for formal recognition as such is still pending. It is obviously important that they be protected from the effects of red notices in the interim, if (per the policy) they are ultimately entitled to be protected from it long-term.

h. **Confidentiality and NDTF decision-making** – INTERPOL's General Secretariat includes seconded staff. NDTF practice seems to involve engagement with NCBs. Currently, individuals (including refugees most at risk of reprisals to them or their families in-country) may be disincentivised from seeking remedies at all due to the uncertainty as to what information is shared by the CCF with IPSG, and what IPSG will discuss with member countries. Current proposals of the CPD, which would apparently mandate the provision of information by the CCF to IPSG, bring this issue very much into focus.

i. **Public extracts of red notices –** INTERPOL arguably creates most damage when it publishes an extract of a notice on its website. The disclosure of information to the public is governed by Article 61 RPD – and INTERPOL should disclose any unpublished policy on this. There ought to be a separate type of CCF challenge available to challenge whether such dissemination is justified, even if one accepts or chooses not to challenge the underlying red notice itself.

26. The above is not the complete list of matters worthy of PACE's attention. Other recent developments may call for scrutiny include e.g. the new Silver Notice (relating to the proceeds of crime); the new Repository of

Practice on Article 2 and 3[13] (which, years overdue, surprisingly fails to mention the flagrant denial of justice standard applied by the CCF); development a new INTERPOL database called INSIGHT offering police forces '***advanced predictive analytics***';[14] and the encouragement to use INTERPOL in a new treaty (infra). The Committee would do well to receive further input from stakeholders on these and other topics.

27. Having regard to the above, I suggest –

    a. The Committee should **encourage INTERPOL to pursue further reforms in the areas identified above**.

    b. The Committee should **receive further input from civil society on INTERPOL** as it considers its draft report and draft resolution.

MLA and TNR

TNR and extradition relations

28. Extradition requests for activists, human rights advocates, journalists etc. may well be cases TNR to the same extent that they involve discrimination and e.g. freedom of expression or conscience issues.

29. It is of course important that Council of Europe states have in place the laws and judicial practice required to both protect against extradition itself, but also (where it is reasonably clear from the outset that an extradition request *is* TNR) to avoid the phenomenon of '*process as punishment*', whereby protracted extradition proceedings and associated rights restrictions achieve the desired effect of TNR even if the person is ultimately protected from extradition.

30. Asylum law represents an important aspect of that. For instance, if activists with other a different residence status become the subject of adverse attention due to activities in the host state, the '*sur place*' basis may require recognition as a refugee,[15] which would potentially preclude extradition proceedings if an extradition request is made later. Criminal allegations in the country of origin may be properly recognised as a basis

---

[13] See the analysis of C. Magri and S. Grossman in *The 2024 INTERPOL Repository of Practice: the unresolved tension between facilitating police cooperation and upholding human rights*, International Bar Association, 2025 (link).

[14] See INTERPOL *Project Insight* (link). Notably, the current brochure (foot of the page) refers to 'advanced analytics' at stage 3 of the project, whereas the original brochure from 2020 refers to 'predictive advanced analytics' under the same stage 3.

[15] See the UNHCR Handbook on Procedures and Criteria for Determining Refugee Status (link) §§94-96.

for recognition as a refugee, prior to any extradition request being made.[16] Another safeguard is the presence of regulated but sufficient discretion for states to decline to pursue extradition requests on behalf of foreign states, where an abuse is obvious or it is doomed to fail.

31. As previously, I suggest –

    a. The Committee should call on **Council of Europe states have in place the full gamut of refusal grounds required to protect against extradition as a form of TNR**, including application of **political or discriminatory motivation grounds** and **ensuring individuals are not exposed to detention resulting from their exercise of their freedom of speech or conscience**.

    b. The Committee should **call on Council of Europe states to have mechanisms in place to avoid subjecting victims of TNR to significant rights restrictions due to incoming extradition requests**, including by considering the asylum implications of foreign interest or allegations before embarking on extradition proceedings; or providing for discretionary powers not to initiate cases which are clearly TNR.

MLA more generally

32. The use of MLA as vehicle for TNR is discussed in a contribution LATR submitted[17] to the Joint Committee of the UK Parliament in its recent inquiry on transnational repression in the UK. I draw on this below.

33. MLA requests are dealt with in a framework of cooperation and thus in a spirit of comity which plays into the exercise of governmental discretion. There is a natural onus on MLA authorities to cooperate. There may be refusal grounds relevant to potential TNR cases, either written in law or derived from treaties, e.g. the ability to refuse cooperation where the proceedings are politically motivated; on human rights grounds; or where data transfers would run contrary to data protection law.

34. However, there is little transparency in relation to the practice of MLA requests. Clearly, if a person is interrogated or their assets frozen, they will know of the MLA. But in many cases, e.g. where the MLA sought is the monitoring of communications or banking information, there will be

[16] As is clearly recognised by Directive 2011/95/EU (refugee qualification directive) (link) Article 9(2)(c) read with Article 10: persecution may take the form of prosecution.

[17] Written evidence of LATR to the Joint Committee (TRUK0148) (link).

no trigger. MLA is dealt with confidentially and, even where individuals seek to proactively warn of potential abuses, MLA authorities may not respond meaningfully as to what they do with the information supplied. There is, therefore, a risk of cooperation with a foreign state's TNR by virtue of the context within which MLA operates.

35. The onus in favour of cooperation finds echo, to some extent, in the ECHR case-law.[18] In the context of TNR, it is important to acknowledge the counterpoint to that, namely that measures taken in execution of MLA requests may engage a Council of Europe state's responsibility under the ECHR, e.g. under Article 8 or Article 1 of the First Protocol.

36. The judgment in Shorazova v Malta[19] spells out that '***mutual legal assistance*** […] ***should be carried out in compliance with international human rights standards*** […] ***domestic courts have an obligation of review where there is a serious and substantiated complaint about a manifest deficiency in the protection of a European Convention right***'. The Court had '*difficulty accepting that the freezing order was in the general interest* [given that] […] ***any such confiscation would result from criminal proceedings which*** *[…]* ***may, or are likely to consist of a flagrant denial of justice.***' Even accepting a general interest in honouring MLA obligations, the Court applied a proportionality analysis with a focus on the duration and effect of restrictions consequent on MLA and procedural safeguards.

37. I would suggest that in cases of MLA requests pursuing an illegitimate TNR purpose, a state may also potentially incur responsibility under Article 18 ECHR together with e.g. Article 8 or Article 1 First Protocol, where it knowingly aids or assists another state in a politically motivated act by restricting a person's rights within its own jurisdiction.

38. It seems obvious, but it is worth stating expressly, that there should be extreme caution with regard to MLA requests which target recognised refugees, particularly where the same state that granted asylum is called upon to execute an MLA request from the country of origin.

---

[18] See e.g. Mukhtarli v Azerbaijan & Georgia 39503/17 (05.09.2024), §155 '*States concerned must take whatever reasonable steps they can to cooperate with each other, exhausting in good faith the possibilities available to them under the applicable international instruments on mutual legal assistance and cooperation in criminal matters.*'.

[19] See Shorazova v Malta 51853/19 (03.03.2022), §111.

39. Where an MLA authority needs a local warrant to carry out a requested measure, such authorities should be bound by a duty of candour to disclose to the court all relevant information about the issuing state's record of TNR.[20] This is a practical means to implement one of the Committee's previous recommendations on this topic.

40. Having regard to the above, I suggest –

    a. The Committee should **recommend that Council of Europe states require MLA authorities to report on (a) number of requests received, from which countries; (b) types of assistance requested; (c) number of requests refused and on what grounds**, such as to permit effective public and parliamentary scrutiny.

    b. The Committee should **recommend that Council of Europe states' MLA authorities follow up on cases in which MLA is provided, and disclose to appropriate (parliamentary or other) authorities where they believe the Council of Europe state has cooperated with a human rights abuse**, e.g. due to regional or international court or other findings relating to the case (or related cases).

    c. The Committee should **emphasise**, per case-law, **that MLA must be implemented consistently with human rights**, including **verifying the presence of genuine public interest** (rather than assuming it because it is MLA); **ensuring the proportionality of any measures** interfering with qualified rights in execution of MLA; **ensuring sufficient procedural safeguards to those affected**; and **not aiding another state in pursuit of an ulterior motive** contrary to Article 18 EHCR.

    d. The Committee should **call for domestic MLA authorities to observe a duty of candour when seeking coercive measures from courts consequent on foreign MLA requests, disclosing pertinent evidence of the requesting state's TNR practices** together with their request.

[20] See in this regard National Crime Agency v Hao & Others [2024] EWHC 2240 (Admin), which at §93 acknowledges the evidence of TNR by China while finding that it was not a concern in the individual case.

The UN Convention on Cybercrime

41. Given current developments in international law, it appears very timely for the Committee to consider the difficult question of the combination of TNR and MLA relating to electronic data and surveillance measures.

42. To provide some context, I would recall two issues. First, the massive abuses associated with the commercial spyware, exemplified by but by no means not limited to NSO's Pegasus software, as discussed in the report of Mr Pietr Omtzigt and associated resolution of PACE, which recognises that commercial spyware may be a key vehicle for TNR.[21] Secondly, the European law saga of Encrochat and Sky ECC, involving the use of hacking capabilities for what have been deemed very successful law enforcement operations, although judicial practice has started to read in some safeguards to the MLA operations involved.

43. These two chapters, side by side, show that there already exists a law enforcement demand for advanced intrusion capabilities,[22] but an equally real demand for such capabilities for malicious purposes, including by governments seeking to abuse them for the purposes of 'digital TNR'. Just as controlling the public procurement and *export* of such capabilities is a key protection against enabling TNR, so there must be protection against *importing* digital TNR via MLA measures.

44. This places in context the most recent developments – in particular with the recent agreement of the UN Convention on Cybercrime ('**UNCC**') in 2024, which will open for signature in perhaps October 2025.

45. The treaty requires law enforcement to have available (Chapter IV) – and to place at the disposal of other states via MLA (Chapter V) – a whole array of powers to capture electronic data, including real-time traffic and content data. It represents the first iteration of standards in this area since the Budapest Convention over 20 years ago, agreed long before the potential scale of use (and misuse) of such capabilities came into focus. The UNCC (if ratified) would inevitably place Council of Europe states in new international legal relations with states known as TNR protagonists.

46. The risk is described by Kate Robertson of Citizen Lab: '*signatories would be required to adopt surveillance and interception capabilities that can be*

[21] Resolution 2513 (2023) Pegasus and similar spyware and secret State surveillance, §14.8.

[22] Prof. Fionnuala Ní Aoláin has indeed observed that the recent Pall Mall Process Code of Practice, while bringing welcome safeguards, assumes legitimate demand for commercial spyware which is 'normalised' to this extent. She observes spyware should be a 'last resort'.

weaponized […] spyware is used as a tool to facilitate transnational repression, or as a repressive end in itself. Repeating mistakes of the past through [the UNCC] *entrenches and worsens these problems*'; [23]

47. Key stakeholders such as Access Now and the Electronic Frontier Foundation consistently criticised flaws in the draft treaty,[24] including the failure to iterate basic norms of data protection law and excessive deference to national laws for safeguards. The flaws are many but illustratively I note two practical safeguards which the states failed to adopt. One proposal was **prior judicial authorisation of the most intrusive measures**: see the opinion of inter alia the UN Special Rapporteur on the Right to privacy while countering terrorism.[25] Another, proposed by inter alia the UN High Commissioner for Human Rights[26] was to require **notification to individuals affected by powers under the UNCC** once the need for confidentiality for effective law enforcement has subsided (without which, the requirement for judicial review is somewhat symbolic). States rejected these in the UNCC, but it remains open to states to adopt such safeguards if they do ratify it.

48. In this regard, it is worth noting that the Draft Third Additional Protocol to the Council of Europe Treaty on Mutual Assistance in Criminal Matters,[27] includes the option for states to make the execution of MLA requests for interception of communications dependent upon certain conditions including '*that, **after the requested interception has taken place**, the authorities of the requested Party **shall** (…) **so inform the subscriber** to the telecommunication service that has been intercepted*'.[28]

49. Given the interest there was in that sort of safeguard in the UNCC negotiations, JUR may wish to explore this further. It is one practical way of achieving effective legal cooperation while enabling individuals to know about measures affecting them and pursue ex post challenges, which would help to identify cases of TNR via MLA. I suggest that JUR might benefit from further input on this from digital rights stakeholders.

---

[23] Kate Robertson, 'A Global Treaty to Fight Cybercrime—Without Combating Mercenary Spyware', *Lawfare*, 22 August 2024 (link).

[24] See the Joint Letter to the EU and its Member States concerning the UNCC (link).

[25] UN Special Rapporteur on the promotion and protection of human rights while countering terrorism, Ben Saul, 25 July 2024 (link).

[26] Submission of OHCHR to the Ad Hoc Committee, 22 July 2024 (link).

[27] COM Request for an opinion Doc. 16139 (25 March 2025), Appendix I (draft treaty) (link).

[28] Article 4(4)(b) of the Draft Third Protocol.

50. I would also like to draw attention to Article 47 UNCC, which requires signatory states to cooperate at a law enforcement level, including via INTERPOL – including with regard to the '*identity, whereabouts and activities of persons suspected*', and the '*movement of proceeds of crime'* – which overlaps with a range INTERPOL blue / red / green / silver notices. The fact of a brand-new UN treaty encouraging use of INTERPOL redoubles the importance of the safeguards at INTERPOL (see supra).

51. Having regard to the above, I suggest –

    a. The Committee should **receive expert input from digital rights stakeholders** so as to further examine the risk of emerging international law inadvertently creating new legal pathways for TNR.

    b. The Committee should **keep a watchful eye on the manner in which Council of Europe states proceed with regard to the UNCC**, both as to signature and ratification (or not) and, if applicable, as to safeguards adopted in domestic implementation measures, especially for those subject to MLA cooperation.

TNR generally

The definition question

52. In its Reply to PACE's last resolution on TNR,[29] the Committee of Ministers asked the Steering Committee on Human Rights ('**CDDH**') to consider the feasibility of a non-binding instrument on TNR, including a definition of TNR. It is unclear what priority that file currently has.

53. Definitions abound and vary significantly. I provide a sample from my own research at Appendix II. In LATR's contribution to the Joint Committee, we called upon the Government to have regard to the work of the Council of Europe when considering the definition issue, the objective being to not miss opportunities to coordinate with partners.

54. A common definition would, at a basic level, help resolve some debated questions, e.g. whether TNR is to be conceived as repression only targeted at diaspora communities themselves or whether it also includes others, e.g. lawyers and journalists of any nationality who cooperate with, work for or support those communities. (I favour the latter.)

[29] Reply to Recommendation Doc. 16114 (5 February 2025) (link).

55. A common definition would also help to pin down the full scope of TNR into a single framework. In this regard, it is instructive to consider the recently released 2023 comparative report[30] of the Swiss Institute for Comparative Law (‘**ICDS**’), dealing with the treatment of TNR in the law and policy of several Western states. The ICDS report grapples with the fact that states may well have policies which tackle certain aspects of TNR, but not necessarily under the guise of any formal or unified TNR policy or even without recognising TNR as such.

56. Indeed, various tactics of TNR may be dealt with in a patchwork of laws on ostensibly unrelated topics, e.g. laws regulating social media; criminal law applicable to espionage and foreign interference or physical assaults; regulation of deep-fakes; asylum law (in particular on sur-place claims); and/or the law on extradition and mutual legal assistance. The needs may vary significantly from place to place, e.g. depending on what diaspora communities live in the host state and what TNR tactics the country of origin employs. TNR practices will also evolve over time.

57. One advantage of a common umbrella definition is that it could provide a general framework for the different forms of TNR and help states to identify gaps in current laws and policies. This would be the all more useful if it was accompanied by the exchange of information between authorities with specific TNR-related mandates, as discussed below.

58. Having regard to the above, I suggest –

    a. The Committee should **continue to call upon CDDH / the COM to come forward with a Council of Europe definition of TNR.**

TNR: a national security and/or rights issue?

59. In the UK context, there has been a discussion as to how TNR is to be conceptualised. The Independent Reviewer of State Threat Legislation asked ‘what planet are we on’ – is TNR a question of national security or one of protecting human rights?[31] He concluded that it was both: the involvement of foreign states in TNR is a national security issue, while from an individual perspective TNR is felt as an interference with rights.

---

[30] Institut Suisse de droit comparé, *Addressing transnational repression: a report on the approaches of Australia, Belgium, Canada, France, Germany, Netherlands, Sweden, United Kingdom, the United States and Italy (addendum)*, 2023/2024 (link).

[31] Independent Reviewer of State Threats Legislation, *Transnational repression: What planet are we on?*, May 2024.

60. The latter aspect should not be under-estimated. Illustratively, Chinese TNR directed at members of Uyghur and Tibetan communities involves a wide array of methods, as documented by, inter alia, Doublethink Lab:[32] cyber attacks and doxxing, affecting both individual data and websites used for activism; direct personal threats and intimidation; threats to families within Chinese territory; or focused disinformation campaigns targeting specific dissidents to undermine their credibility within their communities abroad. All of which may lead to burnout and self-censorship, i.e. successful TNR at the cost of freedom of expression.

61. Further, women are additionally impacted in ways which do not apply to men, in what Citizen Lab has termed gender-based digital TNR[33] which comprises e.g. frequent reports of sexualised online abuse, rape threats, smear campaigns etc. and other tactics with severe personal impact.

62. In this modern TNR context, while prosecutions for national security related criminal offences involving difficult-to-prove state attribution elements are undoubtedly part of the answer, they cannot be the complete solution. Targets also need practical assistance, from technical support with data security issues to psychological counselling.

63. Some recent initiatives and proposals suggest a more holistic approach.

64. In France, the DGSI has launched a TNR webpage[34] which, while well short of the creation of any dedicated agency, at least speaks to a desire for greater accessibility to affected communities and others affected.

65. In the UK, pending the Joint Committee's report, I would note that Dr Andrew Chubb, who focuses on Chinese TNR, in his written evidence proposed the creation of a **Transnational Rights Protection Office** which would be '*tasked with **receiving complaints**, monitoring TNR occurrence, providing **direct support to targets**, advising government on evidence-based policy responses, and liaising with international partners*'[35] – a response to the current approach which has seen TNR reserved to opaque security bureaucracies, leading to an unduly narrow focus on the national security aspect of TNR. Other respondents also

---

[32] Eric Hsu and Ai-Men Lau (Doublethink Lab), *Silenced Voices, Hidden Struggles: PRC Transnational Repression of Overseas Human Rights Activists*, April 2023 (link).

[33] Citizen Lab, *No escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression*, December 2024 (link).

[34] DGSI 'La lutte contre la répression transnationale' (link).

[35] Written evidence of Dr Andrew Chubb (link).

called for a more victim-centre approach to TNR policy, e.g. calling for '*legislative and* ***policy frameworks that put the safety, security and well-being of targeted persons and communities to the fore***'.[36]

66. In the United States,[37] there have recently been proposals in Congress for a Transnational Repression Reporting Act, which would include annual public-facing reports detailing the extent of protective action against TNR;[38] the creation of a Transnational Repression Working Group within the Department of Homeland Security, which would issue annual assessments;[39] another proposal for a public information campaign and research into methods for countering TNR;[40] another for training of public sector agencies and **engagement with exiled communities e.g. as to personal safety practice**.[41] A bill proposed in the California state legislature would require training on law enforcement and make it state policy to protect people from TNR, pursue prosecutions, **provide support to victims**, hold governments accountable and coordinate with Federal level action.[42]

67. In Switzerland, the report of the Federal Council on the situation of Uyghurs and Tibetans in Switzerland noted the need for clarified processes for dealing with TNR; training for authorities; institutionalisation of dialogue with the relevant diasporas; and the necessity of '***un service de conseil facile d'accès pour les victimes et les témoins de la* [TNR]**'.[43] The Swiss parliament's Foreign Policy Committee has now called upon the Federal Council to carry out such measures and propose any legislative steps required to do so.[44]

68. As I see it, the wind appears to be blowing in the direction of a more victim-centred approach, including elements of accessibility and interfacing with affected diaspora communities and victims of TNR.

---

[36] Written evidence of the State Capture Research and Action and the International Partnership for Human Rights (link).

[37] I thank Yuriy Nemets (Washington DC) of LATR for his assistance with US law.

[38] H.R. 9707 (Rep. Schiff) (2023-24).

[39] H.R. 2518 (Rep. Pfluger) (2025-2026).

[40] H.R. 2116 (Rep. G Evans) (2025-2026).

[41] H.R. 2139 (Rep. S Magaziner) (2025-2026).

[42] California State Legislature, 2025/26 session, Senate Bill no. 509 of Sen. Caballero (link).

[43] Report of 12.02.2025 on the situation of Tibetans and Uyghurs in Switzerland (link).

[44] Motion 25.3419 [FR] 'Protection of persecuted communities from influence activities carried out by foreign states'

69. Any non-binding instrument developed by the CDDH / COM would do well to call upon states to adopt that type of approach, including by the creation of specific TNR mandates within the domestic systems. The offices concerned could also exchange knowledge voluntarily between states, minimising blind spots and maximising coordination.

70. Having regard to the above, I suggest –

    a. The Committee should call upon CDDH / the COM to **cover, within proposals for a non-binding instrument** (a) **recommended best practices in all areas of TNR**, (b) **holistic policy** which **include a human rights and victim-centred dimension**; and (c) suggesting **TNR-specific mandates or offices in government** with **the capacity to interface with victims and target communities**.

    b. The Committee should **specifically highlight the position of women subject to TNR with a gendered dimension** and promote policies which mainstream that consideration.

TNR and the legal profession

71. I express solidarity with colleagues at Doughty Street who, for defending Jimmy Lai, have faced multiple forms of TNR including surveillance, interference with their legitimate advocacy within the UN, personal threats and other tactics.[45] The Committee should condemn this.

72. The Council of Europe states recently agreed the new Convention on the Protection of the Profession of Lawyer – which is being signed today (13 May 2025) in Luxembourg. This responds to increasing concern about interferences with lawyers' legitimate exercise of their profession, in particular due to identification of lawyers and their clients.

73. As I read it, that Convention focuses mostly on protection of the legal profession *within* each state party's jurisdiction. It does not appear that TNR was in the forefront of the drafters' minds. That gap can however be met by the Group of Experts under the Convention (called '**GRAVO**') taking account of the issue of TNR as it affects lawyers going forward. It also seems important that bar associations and voluntary lawyers' associations swiftly denounce cases of TNR affecting lawyers.

74. I therefore suggest –

---

[45] 'UK-based lawyers for Hong Kong activist Jimmy Lai targeted by Chinese state', *The Guardian*, 15 February 2025 (link).

a. The Committee should **encourage GRAVO to have regard to the issue of TNR directed at lawyers** in its work under the Convention.

b. The Committee should **encourage bar associations to swiftly come to the defence of lawyers targeted in cases of TNR**.

The Platform to Protect Journalists

75. TNR and journalists is a big topic for another day, and journalists' organisations may have a number of recommendations to make.

76. For now, I note only the fact that the Council of Europe Platform to Protect Journalists[46] does not currently include a 'TNR' category. It may be useful to explore the value of having such a category, which would cover both actual and anticipated TNR, e.g. where new criminal allegations are made. This would ensure that cases of TNR targeted at journalists gain visible recognition as such and help to ensure that host governments consider such cases within the framework of TNR policies and any support and protection practices created thereunder. Further, logically consultation of the Platform should form part of the INTERPOL NDTF's standard open-source research, if it does not already.

77. So, I suggest –

a. The Committee should **consider the potential merit of creating a 'TNR' category within the Platform to Protect Journalists**.

b. The Committee should **invite INTERPOL to confirm that consultation of the Platform to Protect Journalists is part of its open-source work**.

Conclusion

78. I hope that in another 10 years' time, we are not still diagnosing new forms of TNR but measuring tangible the success of the policies adopted to combat it. I thank the Committee for its continued willingness to take on that challenge and will be glad to provide further input.

Alex Tinsley

13 May 2025

[46] *Platform to promote the protection of journalism and safety of journalists* (link).

Appendix I – CPD's proposed revisions of CCF statute

Text of the proposed CCF reforms as presented on INTERPOL's website:

"

The draft amendments to the CCF Statute, currently under discussion by the CPD, are presented below in bold.

Article 33: Examination of requests

1. **The Requests Chamber shall examine an admissible request only after the General Secretariat has taken a final compliance decision on the data concerned.**
2. When a request is considered admissible, the Requests Chamber shall determine whether data concerning the applicant are being processed in the INTERPOL Information System.
3. If no data concerning the applicant are being processed at the time the request is examined, the Requests Chamber may decide on appropriate measures, taking into consideration confidentiality requirements. **The Requests Chamber shall make the information contained in the request available to the General Secretariat so that it may be considered in any future compliance review conducted by the General Secretariat should data be later processed in the INTERPOL Information System.**
4. If data concerning the applicant are being processed in the INTERPOL Information System, and if the request is for correction or deletion, the Requests Chamber shall examine the compliance of the processing of the data with INTERPOL's rules. If the request only concerns access to the data, the Requests Chamber may nonetheless decide to examine the compliance of the processing of those data with INTERPOL's rules. The scope of review of a request shall be limited to examining the compliance of the processing of data with INTERPOL's rules.

Article 37: Provisional measures

1. At any time during the **examination of a request**, the Requests Chamber may decide on provisional measures to be taken by the Organization in relation to the processing of the data concerned.
2. **The Requests Chamber shall not decide on provisional measures before the notification by the General Secretariat of its final compliance decision on the data concerned.**
3. Provisional measures shall be implemented in accordance with the procedure specified in Article 41 of the present Statute.

Article 40: Timeframe for decisions

1. The Requests Chamber shall decide on a request for access to data within four months from the date on which the request was declared admissible, **or the date of notification by the General Secretariat of its final compliance decision, whichever is the later**.
2. The Requests Chamber shall decide on a request for correction and/or deletion of data within nine months from the date on which the request was declared admissible, **or the date of notification by the General Secretariat of its final compliance decision, whichever is the later.**

”

Appendix II – Sample TNR definitions

The below is a sample of 5 definitions of TNR put forward by politicians, civil society, national laws or researchers. For observations on this, see above.

1. Dr Andrew Chubb (2025 evidence to UK Joint Committee) – "***Transnational repression (TNR) refers to attempts by foreign states or proxies to coerce, constrain or punish the exercise of fundamental rights in the UK***"

2. Swiss Federal Council, report on the situation of Uyghurs and Tibetans – ***« on entend par « répression transnationale » l'ensemble des tentatives et des activités transfrontalières d'intimidation ou de répression émanant d'États généralement autoritaires ou non démocratiques. Ces activités visent par exemple des personnes que ces États perçoivent comme une menace. Le but est de les contrôler ou de les faire taire au moyen d'un large éventail de méthodes. Il s'agit donc de réprimer la contestation, l'activisme et l'opposition en créant un climat de peur au-delà des frontières nationales*** »

3. California Legislature, Senate Bill introduced by Senator Caballero – "***Transnational repression is any action taken by government officials, diplomatic personnel, and proxies through acts such as extrajudicial killings, physical assaults, unexplained disappearances, physical or online surveillance or stalking, intimidation, digital threats such as cyberattacks, targeted surveillance and spyware, and online harassment, and coercion such as harassment of, or threats of harm to, family and associates both within and outside the United States.***"

4. House of Representatives, Bill introduced by Adam Schiff – "***The term "transnational repression" means any activity of a foreign government, or an agent of a foreign government or a proxy thereof, that—***

   (A) (i) is any effort to harass, intimidate, or digitally or physically threaten a person to either take action or to refrain from taking action that would be in the interest of the foreign government; or

   (ii) is an attempt to prevent the person from exercising any right that is protected under the First Amendment to the Constitution of the United States, or to retaliate against a person for having exercised such a right; and

(B) targets a United States person or a person in the United States, including through the harassment or intimidation of immediate family members of the person."

5. Freedom House, Policy Recommendations: TNR – "***The term transnational repression describes the ways a government reaches across national borders to intimidate, silence, or harm an exile, refugee, or member of diaspora who they perceive as a threat and have a political incentive to control. Methods of transnational repression include assassinations, physical assaults, detention, rendition, unlawful deportation, unexplained or enforced disappearance, physical surveillance or stalking, passport cancellation or control over other documents, Interpol abuse, digital threats, spyware, cyberattacks, social media surveillance, online harassment, and harassment of or harm to family and associates who remain in the country of origin.***"