Policy Recommendations

For governments of countries that host exiles and targeted diasporas

Improve education and raise awareness about the threat of transnational repression.

- Establish an official definition of transnational repression to be used by all government agencies. This definition should recognize that transnational repression is a threat to democratic institutions and the exercise of individual rights.

- Develop a plan to spread awareness among law enforcement agencies, intelligence services, and officials working with refugees and asylum seekers so that they can incorporate the definition of transnational repression into their procedures, recognize potential perpetrators and victims, and better mitigate and respond to threats.

- Issue travel advisories about states that engage in transnational repression, enabling citizens and residents to make informed decisions about whether and where to travel abroad.

- Develop specific outreach strategies to connect law enforcement agencies with targeted diaspora communities. Inform individuals who are vulnerable to transnational repression of the resources available to them, and learn about different communities’ concerns. Engagement should treat individuals targeted by transnational repression as victims to be protected, not as potential security threats. This outreach should be separate from efforts to counter violent extremism. Although both activities require building community trust, the source and intent of the threat in these two policy areas is quite different. Whenever possible, authorities should distinguish between surveillance and coercion by foreign state agents on the one hand, and indoctrination and recruitment by violent extremist groups on the other.

Limit the ability of perpetrators to commit transnational repression.

- Apply additional vetting to extradition requests and Interpol notices from the governments of countries rated Not Free by Freedom House—and particularly those known to engage in transnational repression—to prevent abuse of law enforcement and judicial processes.

- Review extradition, legal cooperation, readmission and return, and intelligence-sharing agreements with governments that engage in transnational repression. Identify agreements and processes that need additional oversight or that should be discontinued altogether to prevent abuse.

- Screen applications for diplomatic visas to avoid granting accreditation to diplomatic personnel who have harassed, intimidated, or otherwise harmed exiles or diaspora members in the past.

- Restrict the export of surveillance technology. When reviewing export licensing applications, give extra scrutiny to applications from companies seeking to export products to countries whose governments may engage in human rights abuses, especially those previously identified as perpetrators of transnational repression. Where export controls already exist, governments should enforce them thoroughly and update and strengthen them as necessary to account for the development of new technologies.

- Strictly regulate the purchase and use of surveillance tools and protect end-to-end encryption. Government surveillance programs

Track transnational repression and coordinate responses.

- Establish a specific mechanism to track domestic incidents of transnational repression and identify the perpetrator governments. The governments of host countries must create processes to recognize and record cases that occur within their borders. These processes can be built into the existing crime-reporting systems used by law enforcement agencies, but they may require specialized training about the tactics of transnational repression.
should adhere to the International Principles on the Application of Human Rights to Communications Surveillance, a framework agreed upon by a broad consortium of civil society groups, industry leaders, and scholars with the aim of protecting users’ rights. The principles, which state that all communications surveillance must be legal, necessary, and proportionate, should also be applied to open-source intelligence methods such as social media monitoring and the use of intrusive tools such as spyware. To protect the digital security of people targeted by transnational repression, governments should refrain from introducing legislation that weakens encryption, for example by mandating “backdoor” access for authorities or the ability to trace messages.

**Deliver accountability for acts of transnational repression.**

- **Improve targeted sanctions on perpetrators and enablers of transnational repression.** Legislation like the Global Magnitsky Human Rights Accountability Act in the United States provides a mechanism for imposing travel bans and asset freezes on perpetrators of serious human rights abuses. Issuing sanctions for acts of transnational repression in particular would send a strong signal that perpetrators will be held accountable. Countries that possess Magnitsky-style laws should fully enforce them, and countries that lack such legal authorities should enact them. Whenever possible, governments should apply sanctions in a coordinated, multilateral manner for maximum impact.

- **Use persona non grata designations to ensure accountability for transnational repression.** Expel diplomats who are directly involved in transnational repression, or whose governments have committed specific incidents of transnational repression in the host country. Publicly and specifically link the persona non grata designations to individual instances of transnational repression.

- **Restrict security assistance and arms sales to governments that perpetrate acts of transnational repression.** Such governments cannot be trusted to use such assistance responsibly, and they should not be rewarded for violating individual rights and national sovereignty beyond their borders.

**Support victims of transnational repression.**

- **Review the processes for issuing warnings and assigning police protection to individuals, and ensure that they account for the threat of transnational repression.**

- **Commit to respecting the right to seek asylum.** Migration systems should follow the principles set out in the 1951 Refugee Convention. Countries should not create policies with the aim of preventing asylum seekers from accessing their territory. Nor should governments shift the responsibility for asylee processing to third states where people are more vulnerable to transnational repression.

- **Strengthen existing refugee resettlement programs** by including resources to address the threat of transnational repression faced by some newcomers.

- **Limit the use of temporary and subsidiary forms of protection for asylum seekers and instead grant full refugee status.** Such status offers a better safeguard against transnational repression by making the protection permanent, reducing reliance on the origin country for documents, and allowing for family reunification, which reduces the threat of coercion by proxy.

- **Recognize that certain populations experience persecution as a group.** Official recognition would eliminate the obligation to prove individualized persecution in asylum cases.

- **Include details on the use of transnational repression in the information about countries of origin that is consulted during reviews of asylum applications.** Such information would raise awareness among migration officials and help to thwart improper extradition or repatriation requests made by repressive governments.

- **Build resilience against the use of spurious terrorism charges to distort host countries’ asylum and extradition processes.** Fifty-three percent of cases of physical transnational repression involve accusations of terrorism, which allow origin states to exploit the security concerns of host states and persuade them to unjustly detain and deport targeted individuals. These accusations often tap into existing xenophobic and Islamophobic biases in host countries. Governments should review migration practices to identify areas where policies focused on combating violent extremism and terrorism effectively view people as potential security threats rather than potential victims and thus overlook the risk of complicity in transnational repression.
• Fund civil society organizations that monitor incidents of transnational repression or that provide resources to targeted individuals and groups. Ensure that civil society work on both digital and physical forms of transnational repression receives adequate and sustainable financing.

For civil society

• Invest in digital hygiene trainings and make resources on digital security widely accessible to targeted communities, reaching beyond professional activists and journalists. Where the community includes refugees, digital hygiene should be integrated into refugee resettlement programs. Digital hygiene training should include incident response planning, which allows people to prepare for the steps they should take if they suspect that their digital security has been compromised.

• Continue to document incidents of transnational repression, analyze perpetrator states’ tactics, and identify gaps in policy responses. Civil society groups often have unique, on-the-ground sources of information and are a key point of contact for affected individuals. By sharing their data and analysis with the media and policymakers, they can improve public awareness and prompt more effective government action.

• Develop programming for individuals affected by transnational repression, including social, psychological, legal, and immigration support. Such support should be tailored to the needs of specific diaspora communities, and it should include both harm remediation and tools for pursuing accountability.

For UN member states

• Recognize transnational repression as a specific threat to human rights and work with like-minded governments to establish norms and develop multilateral responses.

• Review and revise the protections that are offered to human rights defenders and other activists who engage with the UN to better address the risk of transnational repression. The current safeguards have failed to prevent some governments from excluding, intimidating, or punishing dissidents when they attempt to participate in UN processes.

• Establish a special rapporteur for transnational repression. Existing rapporteurs and working groups lack the mandate required to provide a comprehensive picture of the problem.

For technology companies

• Create a company-wide strategy to respond to transnational repression. Raise internal awareness and provide training on the tactics of transnational repression to avoid unwitting complicity. Relevant policy areas may include but are not limited to content moderation, harassment, foreign influence operations, cybersecurity, and privacy. Companies should develop expertise in the languages of targeted communities, work with civil society to identify individuals who may be at risk of online threats or harassment, engage with such individuals or groups to understand their needs, and share best practices with peer companies.

• Adopt secure protocols like end-to-end encryption for company products and expand special protections and safety settings for people who are vulnerable to transnational repression. Companies should proactively notify users who are at risk of or have already suffered from digital attacks and offer resources on how to protect accounts. They should also cooperate with civil society to engage in outreach and draw more people into their digital hygiene programs.

• Strengthen options for documenting transnational repression on digital platforms. It should be recognized that documentation is often burdensome and traumatizing for individuals, but also crucial to civil society research and law enforcement activity. Consider giving people access to tools that allow them to filter, review, report, and document transnational repression in a convenient way. Develop internal means of documenting incidents that can be used to inform company policies. Any form of documentation should prioritize user privacy.

• Publicly identify perpetrators of digital transnational repression and describe the methods and scale of their activity. Insofar as such revelations do not expose victims to further harm. Consider standardizing this reporting, for instance by including it in regular reports on transparency, human rights, or foreign influence operations.