

Countering Transnational Repression (TNR): Component of an Effective Response

Main Vectors

<p>Direct attacks:</p> <ul style="list-style-type: none"> • Harassment, threats, and intimidation • Assault • Detentions and arrests • Involuntary returns • Attempted assassinations and/or assassinations 	<p>Long distance threats:</p> <ul style="list-style-type: none"> • Cyber threats, harassment, and intimidation • Coercion-by-proxy 	<p>Mobility controls:</p> <ul style="list-style-type: none"> • Denying the ability to leave the country • Forcing victims to return • Controlling travel documents • Forcing victims to appear at consulates or embassies in host countries 	<p>Co-opting other countries:</p> <ul style="list-style-type: none"> • Many states do not respect the principle of non-refoulement • Denial of entry to victims based on false accusations of perpetrator state
---	---	--	--

Diplomatic Tools

Proactive bilateral & multilateral collaboration

<p>Public Comms & StratComms:</p> <p>GAC Comms counter disinformation on public platforms, often providing both counter-narratives and advice and guidance for detecting disinformation</p>	<p>Public Attribution of hostile activities:</p> <p>Symbolic gestures to votes by the legislature and public 'naming & shaming' of specific actors. The GAC-led GoC public attribution framework guides recommendations on attribution.</p>	<p>Cancelling visits, taking retaliatory measures:</p> <p>Issuing demarches, planning or cancelling high level visits. Taking retaliatory measures to reduce or limit performance of Canada's obligations under Canada's agreements.</p>	<p>Curtailing diplomatic engagement, denying visas:</p> <p>GAC manages privileges and immunities of foreign diplomats. Important tool, notably in cases where foreign states seek to use accredited diplomats to conduct interference activities.</p>	<p>Sanctions:</p> <p>Part of the toolkit to respond to malicious behaviour, including in information manipulation campaigns, acts of TNR, etc.</p>	<p>International Engagement to support Human Rights Defenders (HRD):</p> <p>Multilateral fora to strengthen international rules, norms, human rights; bilateral diplomacy to engage local authorities; partnerships with states, civil society, Indigenous peoples & the private sector, including Canadian business interests abroad, to build capacity; responsible business conduct.</p>	<p>G7 Rapid Response Mechanism:</p> <p>Threat intelligence sharing with governments; Early flagging of content and behaviours to affect adversarial activities; New TNR WG to raise TNR profile globally and develop best practices & work together to counter TNR.</p>	<p>Bilateral coordination and partnerships:</p> <p>Support to organizations and networks working on detection, fact-checking, prebunking, awareness and literacy, capacity building and others aimed at preserving information integrity and raising resilience.</p>	<p>Multilateral coordination:</p> <p>Development of international frameworks, norms and practices; Shaping international rules for responsible behaviour in the digital environment; Engaging with strategic partners and 'neutrals' to counter authoritarian visions for the global information environment.</p>
--	--	---	--	---	--	--	---	--

TNR is a subset of Foreign Interference

<p>Definition</p>	<p>It describes the acts by governments, either direct or through proxies, to silence, intimidate and/or exact reprisal against groups and individuals and/or their families perceived as threats, outside their sovereign borders, including members of diaspora populations, political opponents, civil society activists, religious/ethnocultural groups, human rights defenders, and journalists. These acts also include instrumentalization of diaspora through intimidation of diaspora members to cooperate with the perpetrator state and harassment of or harm to family and associates who remain in the country of origin.</p> <p>Methods and tactics of transnational repression include, but are not limited to assault, abduction, detention, rendition, forced disappearances and even assassination; extraterritorial threats and coercion, including malicious cyber activities; physical and online surveillance and harassment over digital platforms including through commercial spyware; mobility controls, such as passport confiscation or denial of consular services; use of other states or international institutions to facilitate the detention or forced return of targeted individuals; the misuse of counterterrorism tools, such as information sharing-arrangements; and the misuse or attempted misuse of INTERPOL systems.</p>
--------------------------	--

