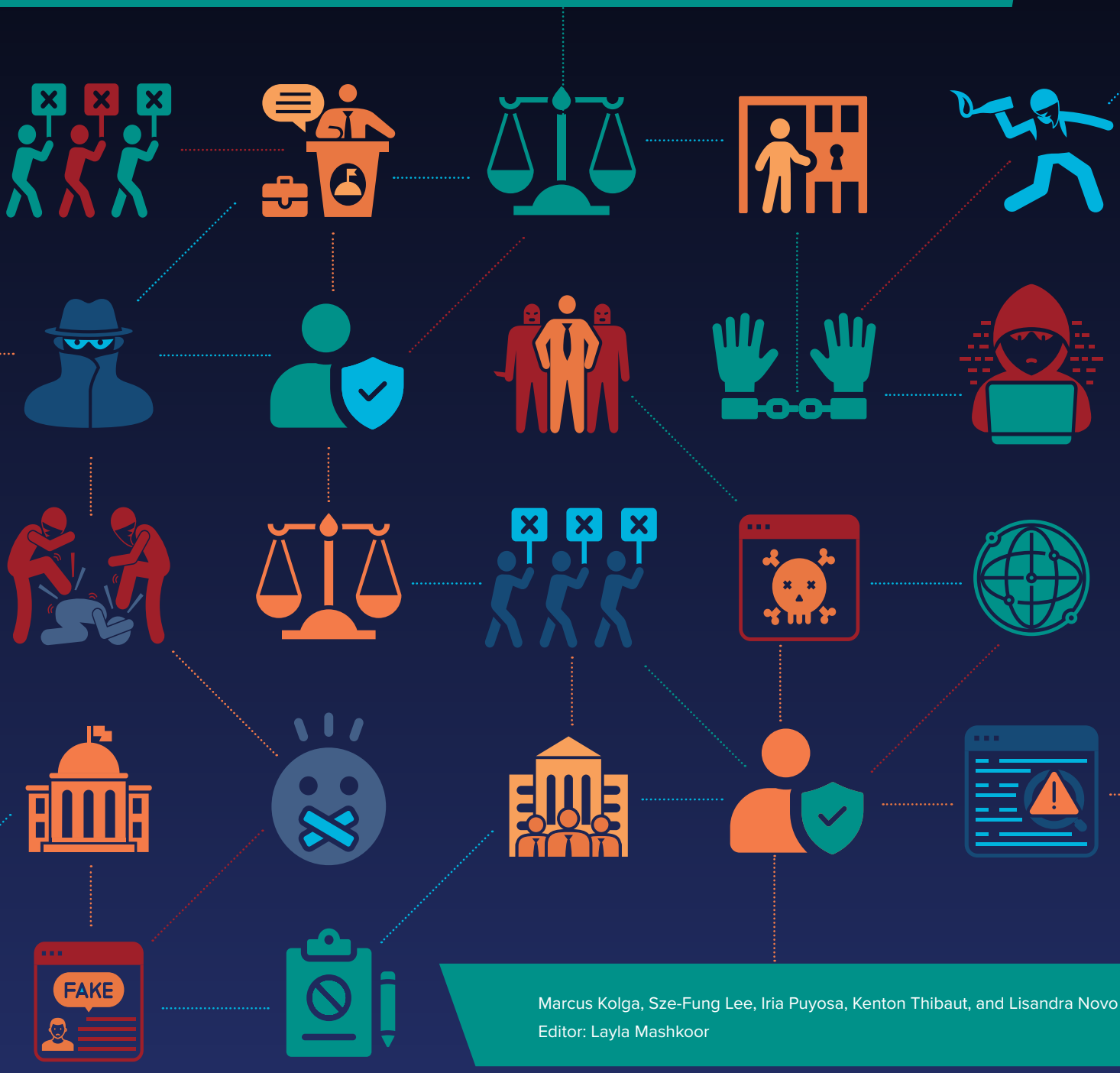
Atlantic Council DFRLab

Authoritarian reach and democratic response:

A tactical framework to counter and prevent transnational repression



Marcus Kolga, Sze-Fung Lee, Iria Puyosa, Kenton Thibaut, and Lisandra Novo
Editor: Layla Mashkoor

The mission of the Digital Forensic Research Lab (DFRLab) is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

Cover: Donald Partyka

Please direct inquiries to:

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

ISBN: 978-1-61977-603-6

Authors

Marcus Kolga
Sze-Fung Lee
Iria Puyosa
Kenton Thibaut
Lisandra Novo

Editor

Layla Mashkoor

Atlantic Council

DFRLab

Authoritarian reach and democratic response:

A tactical framework to counter and prevent transnational repression

Table of contents

Executive summary

- **Foreign interference (FI) and transnational repression (TNR) represent a fundamental challenge to the international rules-based order by employing tactics that exist below the threshold of armed conflict while violating national sovereignty.** Beyond national borders, authoritarian states have targeted policymakers, elected officials, researchers, journalists, activists, and diaspora communities worldwide to advance their political objectives. These TNR tactics encompass cross-domain operations, including surveillance, cyberattacks, disinformation, legal and judicial harassment, and physical and psychological assault.
- This report introduces a comprehensive framework to analyze FI and TNR tactics, techniques, and procedures (TTPs) and to propose actionable responses, which we refer to as countermeasures, to disrupt, deter, and prevent future operations at various stages.
- Case studies on Chinese and Russian TNR activities demonstrate how this framework could be employed and how different entities—whether international or domestic, governmental or civil—can adopt practical countermeasures at each stage of operations.
- Designed to empower domestic and international governmental organizations, along with law enforcement and intelligence agencies, civil society, media, and vulnerable communities, this framework provides a structured blueprint that outlines specific roles and strategies, as well as how different entities can collaborate to counter TNR threats. The ultimate goal is to establish a global, whole-of-society approach that fosters collective responses across like-minded democracies.

Introduction

TNR represents a growing threat to democratic societies worldwide, as authoritarian regimes extend their repression beyond borders, utilizing covert and overt influence operations to advance their political objectives. Over the past decade, the term "transnational repression" has been used to describe the actions of states that seek to control populations living outside their borders. University of Notre Dame Professor Dana M. Moss coined the term to refer to "the repression of diasporas by home-country regimes," which aims to "punish, deter, undermine, and silence activism in the diaspora," thereby preventing these populations from completely exiting authoritarian control.[1]

State, state-affiliated, and non-state actors employ a range of coercive strategies to silence critics, alienate opposition, and control diaspora communities via intimidation. TNR manifests into a sophisticated blend of operations, including surveillance, cyberattacks, disinformation campaigns, legal and judicial harassment (sometimes called lawfare), and even physical and psychological assault. As these operations often exist in legal gray zones, they exploit vulnerabilities within liberal democracies, challenging the international rules-based order below the threshold of major pushback from the international community. Despite growing efforts and attention toward the issue, democracies have struggled to counter these extraterritorial repression tactics effectively.

The use of undercover agents and proxies to intimidate critics and pro-democracy activists is a tactic that allows malign state actors to retain a certain level of deniability. Moreover, gray-zone operations exploit the limitations of law enforcement—specifically its capacity, capabilities, and legal mandate—to adequately support victims of transnational repression. These operations also take advantage of legal gaps and loopholes that hinder the investigation of threats and prevent the prosecution or detention of perpetrators, particularly in cases where the situation has not yet escalated to physical violence.

When foreign governments conduct surveillance, intimidation, or enforcement actions—including through the exercise of extraterritorial police power by authoritarian regimes inside the nations they target—they undermine state sovereignty and threaten to erode public trust in institutions, representing a significant national security threat.

A strategic framework on transnational repression is urgently needed to confront this rapidly evolving global threat. While the body of research and policy responses has been slowly developing over recent years, these actions remain largely fragmented, reactive, and uncoordinated. What is lacking is a unifying, practical framework that consolidates these efforts and provides a comprehensive, proactive approach to understanding, disrupting, preventing, and countering transnational repression.

As resources to support activists, journalists, and diaspora communities targeted by TNR come under increasing strain—exacerbated by the growing absence of sustained US leadership and funding in this domain—the need for a common strategic framework is more urgent than ever. In this context, a unified framework to guide Western democratic allies will foster greater coherence and coordination, while also supporting the accelerated development, implementation, and effectiveness of policies and countermeasures. By providing a shared foundation for identifying threats, protecting vulnerable communities, and confronting the foreign regimes that engage in TNR, such a framework would strengthen collective democratic resilience at a time when it is most critically needed. Ultimately, the goal is to establish a global, whole-of-society approach that fosters collective responses across like-minded democracies.

The framework we propose draws and builds upon pre-existing structures developed to counter cyber threats and disinformation, including Mitre's ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) Framework,[2] the DISARM Foundation's DISARM (Disinformation Analysis and Risk Management) Framework,[3] and Meta's Online Operations Kill Chain,[4] among others. These foundational models provide tested conceptual and operational tools for understanding threat actor behavior, information manipulation, and harm mitigation in the digital space.

The Citizen Lab and Freedom House have contributed conceptually and methodologically to studying TNR. The Citizen Lab has been influential in debates on digital authoritaria-

1. Dana M. Moss, "Transnational Repression, Diaspora Mobilization, and the Case of the Arab Spring," *Social Problems* 63, 4 (2016), 480–498, https://academic.oup.com/socpro/article/63/4/480/2402855.
2. AttackIQ, "MITRE ATT&CK Matrix," AttackIQ, accessed September 30, 2025, https://www.attackiq.com/mitre-attack/matrix/
3. DISARM Framework Explorer, "DISARM Frameworks," accessed September 30, 2025, https://disarmframework.herokuapp.com/
4. Ben Nimmo and Eric Hutchins, *Phase-based Tactical Analysis of Online Operations*, Carnegie Endowment for International Peace, March 16, 2023, accessed September 30, 2025, https://carnegieendowment.org/research/2023/03/phase-based-tactical-analysis-of-online-operations?lang=en

nism and has pioneered research on digital TNR, defining it as governments using "digital technologies to surveil, intimidate, and silence exiled dissidents and diaspora communities."[5]

Its research explores the methods and impacts of digital TNR, drawing on qualitative data including interviews with targeted individuals such as human rights defenders, journalists, and dissidents living in exile. The Citizen Lab's work has highlighted impacts such as self-censorship, psychological harm, and the erosion of community networks.

Freedom House, in turn, has conducted global studies of TNR, defining it as "reaching across borders to silence dissent among diasporas and exiles through a variety of methods, including assassinations, deportations, abductions, digital threats, Interpol abuse, and family intimidation."[6] It has created publicly available databases that document incidents of TNR based on public sources and interviews, providing a picture of this global phenomenon and identifying perpetrator states. Freedom House emphasizes that transnational repression is a "daily assault on civilians everywhere — including in democracies like the United States, United Kingdom, Canada, Germany, Australia, and South Africa" and a serious threat to human rights, democratic institutions, and state sovereignty.[7]

By adapting these established methodologies to the unique characteristics of TNR—including state-sponsored harassment, surveillance, intimidation, and coercion targeting diaspora communities and human rights defenders—this framework acknowledges the evolving, hybrid nature of authoritarian tactics that blend information warfare with direct offline threats.

Rather than reinventing an entirely new architecture, the objective of this framework is to extend and enhance the utility of existing frameworks by tailoring their components to the specific dynamics of global TNR. This includes integrating elements that account for current policy gaps, diaspora vulnerability mapping, coordinated policy responses, and civil society resilience.

By understanding the objectives and TTPs of transnational repression, this project aims to propose actionable countermeasures to disrupt, deter, and prevent future TNR operations at various stages through a comprehensive framework.

5. Noura Al-Jizawi, et al., "Psychological and Emotional War: Digital Transnational Repression in Canada," *Citizen Lab Research Report* 151 (2022), https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/.

6. Freedom House, "Transnational Repression: Understanding and Responding to Global Authoritarian Reach," Freedom House, accessed September 30, 2025, https://freedomhouse.org/report/transnational-repression

7. Freedom House, "Transnational Repression," last visited October 2, 2025, https://freedomhouse.org/report/transnational-repression

Key components

1. **Prevention and awareness:** The framework empowers at-risk communities with knowledge and tools to recognize and mitigate threats. This involves targeted awareness and education on digital security, operations security, and psychological resilience, as well as the creation of accessible and integrated reporting mechanisms for incidents of TNR.
2. **Intervention and disruption:** The framework strengthens intelligence and law enforcement cooperation at all domestic levels and internationally, increasing interoperability to identify and dismantle networks and TNR operations. Community-based rapid response teams and collaborative monitoring of social media platforms play critical roles in minimizing harm during active operations.
3. **Accountability and deterrence:** The framework provides for the implementation of targeted, defensive sanctions (in contrast to sanctions deployed by foreign regimes as part of TNR) against perpetrators and collaborators who have been exposed and leveraging international legal frameworks to hold regimes and their enablers accountable. Public awareness campaigns and partnerships with civil society groups and investigative media organizations can also ensure transparency and deter future operations.
4. **Victim support and rehabilitation:** Victims of TNR often suffer various degrees of debilitating psychological trauma.[8] Providing psychological counseling, legal aid, and resources for victims to rebuild their lives and reputations,[9] while fostering solidarity among those affected, is a key recovery component for victims.

Over the past decade, authoritarian regimes have escalated their efforts to surveil, intimidate, and punish policymakers, journalists, academics, activists, and diaspora communities living in democratic states, solely for exercising their fundamental rights to dissent. The cumulative impact on victims—ranging from psychological trauma to reputational harm and exclusion from public life—is both profound and destabilizing. No individual or institution is entirely immune to the risk.

The development of a multilateral coalition of democratic nations committed to coordinated action against authoritarian interference is needed to address this threat. Through mechanisms such as shared intelligence, joint investigations, and harmonized diplomatic initiatives, such a coalition would serve as a structured platform to defend democratic values and protect individuals and communities targeted by TNR.

Although existing efforts such as the Freedom Online Coalition and the Media Freedom Coalition have sought to address elements of TNR, they often lack the mandate, operational cohesion, or enforcement capacity to counteract the increasingly sophisticated and extraterritorial nature of authoritarian tactics.

When combined with the framework presented in this report, a coalition of allied democracies can fill the critical gap in the current global response by establishing an institutionalized, collective defense mechanism that is both preventive and responsive. Such a coalition would establish clear protocols for information sharing, applying a unified framework for identifying and documenting instances of transnational repression, and coordinating diplomatic and legal measures to hold perpetrators accountable.

Key terms

Transnational repression (TNR): We expand on Freedom House's aforementioned definition and place the use of TNR in the context of broader foreign information manipulation and interference (FIMI) operations. We highlight the use of covert and overt influence operations and TTPs by state, state-affiliated, and non-state actors to advance political objectives abroad. Tactics include silencing critics, alienating opposition, controlling diaspora communities via intimidation, and techniques updated to highlight digital means, including surveillance, cyberattacks, and disinformation campaigns, as well as legal and judicial harassment (lawfare), and physical and psychological assault.

Digital transnational repression: This refers to the use of digital technologies by authoritarian states to surveil, harass, intimidate, or silence dissent beyond their borders. As documented by the Citizen Lab and Freedom House, this practice includes tactics such as spyware deployment, online harassment, phishing, and coordinated disinformation targeting

8. Alexander Chipman Koty, "Three Things Canada Can Do To Address Transnational Repression," *Digital Public Square*, August 25, 2025, accessed September 30, 2025, https://digitalpublicsquare.org/insights/three-things-canada-can-do-to-address-transnationa/
9. Yana Gorokhovskaia, Nate Schenkkan & Grady Vaughan, *Still Not Safe: Transnational Repression* in 2022 (Washington, DC: Freedom House, April 2023), accessed September 30, 2025, https://freedomhouse.org/sites/default/files/2023-04/FH_TransnationalRepression2023_0.pdf

exiles, diaspora communities, and human rights defenders.[10] This allows them to exploit interconnected digital infrastructures to extend state repression beyond their borders.

Influence operations: In the context of FIMI, influence operations refer to coordinated efforts by state or non-state actors to shape public opinion, political decisions, or social dynamics to align with their strategic interests.[11]

Information operations: Information operations involve the targeted manipulation of the information environment—such as disseminating disinformation, disrupting communication channels, or degrading trust in institutions—to facilitate broader influence goals. Information operations are thus often a tactical component within influence operations. While influence operations focus on altering perceptions and behaviors, information operations primarily manipulate the medium through which those perceptions are formed.[12]

Foreign influence: Foreign influence refers to efforts by a foreign actor to shape public perceptions, political discourse, or policy outcomes in another country through legitimate, transparent, and often lawful means, such as diplomacy, public messaging, or cultural engagement.[13]

Foreign interference: In the context of FIMI, foreign interference involves covert, coercive, deceptive, or corrupt activities intended to disrupt or subvert a target country's political processes, public opinion, or societal cohesion. While foreign influence is a routine aspect of international relations, foreign interference crosses normative and legal boundaries by seeking to manipulate domestic systems without the target's informed consent.[14]

Lawfare: This refers to the strategic misuse of legal systems and processes to achieve political or coercive objectives. Authoritarian states and their proxies may employ lawfare to silence or intimidate critics abroad through abusive lawsuits known as **strategic lawsuits against public participation (SLAPPs)**, or by exploiting extradition mechanisms, defamation laws, and other judicial tools to harass, discredit, or exhaust their targets.

The following pages present a global strategic framework for understanding and countering TNR. This framework traces the full arc of TNR operations, from planning and preparation to execution, outlining the key stages, tactics, and actors involved. For each phase, it identifies strategic entry points for countermeasures aimed at disrupting, deterring, and ultimately preventing these campaigns. Designed to be geographically agnostic, the framework is intended for application across jurisdictions and contexts. It offers practical tools for governments, civil society, and at-risk individuals or communities to anticipate threats and strengthen their resilience against authoritarian reach beyond borders.

10. "Digital Transnational Repression," Citizen Lab, last visited May 22, 2025, https://citizenlab.ca/category/research/targeted-threats/dtr/; Marcus Michaelsen, "The Digital Transnational Repression Toolkit, and Its Silencing Effects," Freedom House, July 2020, https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its-silencing-effects.
11. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (New York: Farrar, Straus and Giroux, 2020); U.S. Office of the Director of National Intelligence (ODNI). 2021. "Foreign Threats to the 2020 US Federal Elections," National Intelligence Council, March 10, 2021, https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.
12. "Summary of the Department of Defense Cyber Strategy," US Department of Defense, September 2018, https://dodcio.defense.gov/Portals/0/Documents/Library/CyberStrategy2018.pdf .
13. "Foreign Threats to the 2020 US Federal Elections"; Christopher Walker, "What Is 'Sharp Power'?" *Journal of Democracy* 29, 3 (2018), 9–23, https://www.journalofdemocracy.org/articles/what-is-sharp-power/.
14. Countering Foreign Interference in Australia," Australian Government Department of Home Affairs, 2024, https://www.homeaffairs.gov.au/nat-security/files/cfi-australia.pdf.

Groups most vulnerable to transnational repression

Dissidents and exiles from authoritarian states

Exiles are pursued through a blend of legal theatrics and covert intimidation. Fabricated charges, Interpol notices, and extradition requests manufacture a sense of perpetual jeopardy. Agents and informants try to penetrate exile groups to identify backers, safe houses, and vulnerable relatives. Offers of amnesty or reconciliation promise safety while coaxing addresses, travel plans, or a return that ends in detention. Digital operations range from spyware and SIM swaps to social engineering through respected community figures. Financial life is targeted as well: bank accounts are closed, property is seized, and employers or landlords receive quiet warnings, all of which sap stability and dampen political activity.

Civil society, frontline human rights activists, and human rights lawyers

Authoritarian states focus first on the people who move communities and shape policy. Frontline advocates are harassed online, tracked through commercial spyware, and smeared to discredit their campaigns. Complaints to employers and funders are used to choke off resources, while venue pressure aims to cancel public events. Families in the origin state face threats to jobs, property, or personal safety, which creates powerful leverage to silence organizers abroad. Human rights lawyers are most exposed when their work is public or tied to high-profile cases, drawing similar harassment and lawfare. Travel to third countries brings risks of surveillance, device searches, and denial of entry and/or re-entry, often wrapped in bureaucratic pretexts that are difficult to contest.

Journalists and media workers

Independent reporting exposes abuses and holds regimes to account—making journalists significant targets of information and influence operations and direct digital intrusion. Orchestrated smear dossiers and manipulated media attempt to poison the reputation of editors and turn audiences against them. Phishing, credential theft, and device compromise threaten sources and story pipelines. Proxies with diplomatic cover plant and promote counter-narratives to chill coverage, while relatives in the origin state receive "warning" calls that raise the cost of continued reporting. Freelancers, fixers, and photographers are especially vulnerable at borders and airports, where devices can be searched and contacts copied. Legal threats and takedown demands create ambient risk that nudges newsrooms toward safer assignments and away from sensitive investigations.

Minority ethnic and religious diaspora groups

Diaspora communities often carry living ties to people and property in the origin state, which gives authoritarians a grip they exploit. Consular staff and affiliated associations monitor protests, cultural gatherings, and places of worship, then contact family members to apply pressure. Messaging app check-ins and requests for "updates" on peers normalize surveillance inside the community. Propaganda frames cultural pride as extremism, stigmatizing participation and spooking venues and donors. Infiltration of student and community groups helps map leadership, finances, and attendance lists. The result is a steady erosion of trust that discourages collaboration with local authorities, journalists, and schools, and slowly narrows the public space for cultural life.

Women, LGBTQI+ individuals, and children

Gender and sexuality are often grounds for persecution exploited by origin states engaging in transnational repression. The Citizen Lab has published novel research on the various ways in which gender is weaponized as a tool of digital transnational repression against human rights defenders, journalists, civil society, and other targeted groups.[15] Women and LGBTQI+ individuals face additional specific threats based on gender identity and sexual orientation that lead to disproportionate harms and technology-facilitated gender-based violence. Harassment often involves threats of sexual violence, sexist insults, and derogatory comments about their bodies or physical attributes.

Children are also especially vulnerable as not only are they victims of the violations against their parents, guardians, or adult caretakers, but can become targets themselves as part of the campaign of repression against the adults in their lives. For example, the son of one woman human rights defender received explicit images online and threats to assault his mother in front of him as part of the campaign against her.[16] In another instance, a woman journalist reported that while conducting advocacy before the UN in Geneva, not only was she harassed and threatened, but she received threats directly against her children.[17] These tactics, whether digital or physical, serve

15. Noura Aljizawi, et al., "No Escape: The Weaponization of Gender for the Purposes of Digital Transnational Repression," *Citizen Lab Research Report* 180 (2024), https://citizenlab.ca/2024/12/the-weaponization-of-gender-for-the-purposes-of-digital-transnational-repression/.

16. Ibid.

17. Saipira Furstenberg, et al., "Transnational repression of human rights defenders: The impacts on civic space and the responsibility of host states," *European Parliament Study* (June 2025), https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2025)754475.

the same purpose: to intimidate these groups and silence them through fear for themselves or their children.

Students, scholars, and campus communities

Universities are fertile ground for pressure because visas, funding, grades, and career prospects can be leveraged at once. Surveillance within student associations and the casual recording of classes chill debate before it begins. Letters to administrators accuse student organizers of extremism, triggering investigations or event cancellations that drain energy and time. Foreign students fear immigration or academic consequences if they speak out, while researchers working on sensitive topics face hacking, data theft, and travel risks around conferences or fieldwork. Attendance lists and photographs of campus events are relayed to the origin state, where they are used to intimidate students and their families.

Elected officials, policymakers, and political staff

Lawmakers are pressured through calibrated reputational threats and manufactured community backlash. Forged correspondence, deepfakes, and choreographed complaint campaigns aim to spook ethics officers and party whips. Front groups mimic grassroots sentiment to frame sanctions, transparency registries, or human rights motions as assaults on constituents. Staffers and relatives may be targeted with hacked or selectively leaked communications to create scandal pressure. Courting of local donors and cultural leaders provides a respectable face to coercion. The cumulative effect is to shift agendas, slow hearings, and dilute statements at precisely the moments when clarity is most needed.

Refugees, asylum seekers, and recent migrants

People rebuilding their lives carry the heaviest burdens and the fewest protections. Demands to visit consulates, document manipulation, and social media "assistance" that turns into entrapment exploit uncertainty about rights and procedures. Informal community gatekeepers sometimes report activism back to security services. Threats to relatives, remittances, or property discourage testimony and public advocacy. Rumors seeded in community channels can isolate individuals and make landlords or employers wary. Fear of jeopardizing a refugee or asylum claim keeps many from contacting police or NGOs after incidents, allowing harassment to continue in the shadows while simultaneously fraying trust in local institutions.

Cultural and religious institutions and community organizations

Cultural life provides public visibility, which makes institutions convenient pressure points. Infiltration of boards, sudden venue cancellations, and coordinated complaint campaigns disrupt programs and dishearten volunteers. Propaganda casts festivals, memorials, and religious gatherings as political agitation, chilling attendance and sponsorships. Clergy and community elders receive "friendly" outreach that leverages relatives abroad to influence programming choices. Online mobs and bomb threats raise security costs beyond what small organizations can bear. Systematic photo documentation of attendees is used to map networks, identify organizers, and intimidate families, reducing the willingness of communities to gather in public settings.

Tech platform trust and safety staff, OSINT researchers, and content moderators

Those who expose covert networks or advocate for the enforcement of platform rules against state actors may be targeted to intimidate other experts. Doxxing, threats, phishing, and deepfake harassment attempt to intimidate them into silence and deter their peers. Data brokers and breached databases are mined to surface home addresses, relatives, and daily routines. Legal demands push for takedowns or disclosure of methods and sources, while public pressure campaigns allege bias to hobble enforcement against coordinated inauthentic behavior.[18] Smaller teams with high visibility and limited security support are especially vulnerable to burnout, which is itself an objective: fewer eyes on the problem means fewer obstacles to the next operation.

18. "Inauthentic Behavior," Transparency Center, Meta, accessed September 30, 2025, https://transparency.meta.com/policies/community-standards/inauthentic-behavior/

Whole-of-society roles for democratic defense

Countering transnational repression demands a whole-of-society approach. Roles across institutions, communities, and individuals must be clearly defined and aligned to confront authoritarian threats effectively. This means activating civil society, NGOs, law enforcement, parliamentarians, community leaders, elected officials, and the media to provide early warning, support victims, disrupt operations, deter perpetrators, and secure accountability. Clear mandates, practical resources, and rapid coordination can help turn awareness into protection—and protection into deterrence.

Civil society and NGOs (human rights, digital security, grassroots, diaspora associations, community groups, etc.)

Early warning and trust building:

- Organize awareness campaigns and materials;
- Identify and map out front groups, proxies and enablers, sharing with other groups such as law enforcement;
- Identify vulnerable individuals to aid in early detection of threats;
- Facilitate coordination and trust building initiatives between stakeholders, community groups, law enforcement and government.

Capability building:

- Digital hygiene trainings, platform reporting guides, and security audits for community organizations;
- Briefings for journalists, elected officials, NGOs, and community leaders.

Information collection and sharing:

- Develop robust informed consent protocols for collecting information from victims and witnesses;
- Develop clear data access protocols when sharing information with any other stakeholders based on parameters of informed consent;
- Document cases and build secure databases;
- Create incident briefs for government, NGOs, and police subject to informed consent restrictions and data access protocols;
- Issue community risk bulletins in anticipation of emerging issues, protests, festivals, or high-profile visits.

Victim support:

- Advance safety awareness and planning in partnership with community, civil society organizations, and law enforcement;
- Education on secure evidence capture (screenshots with metadata, archiving of online harassment, call logs, message exports) and on risks of holding such evidence;
- Develop pathways to report incidents to relevant law enforcement and government agencies, as well as civil society groups and social media companies;
- Assistance in evidence preservation in accordance with applicable chain of custody requirements by civil society organizations and law enforcement;
- Psychological support and rehabilitation of reputations.

Case intake and triage:

- Standardized forms, risk scoring, and chain-of-custody for digital and physical evidence;
- Emergency micro-grants for phones, locks, relocation, or counseling.

Escalation and advocacy:

- Assist in evidence preparation;
- Pursue strategies to defend against SLAPPs, sanctions listings, visa bans;
- Publish periodic TNR trend reports.

Community leaders and institutions (faith-based, cultural, campus, business associations)

Safeguarding:

- Speaker and sponsor vetting;
- Event attendee responsibility and privacy rules;
- Vetting of any potential funders.

Gatekeeping against infiltration:

- Broad conflict-of-interest disclosures, access controls to mailing lists and membership rolls, periodic security reviews.

Liaison and coordination:

- Identify and name contacts for police and NGOs;
- Routinize post-event debriefs and threat pattern sharing.

Law enforcement and security services (local police, national security, border control)

Structure and training:

- Establish dedicated TNR points of contact in major cities and dedicated experts;
- Develop routine patrol and intake training on TNR threats;

- Adopt proactive policies to identify and disrupt harassment that falls below the criminal threshold, using early intervention, civil remedies, and platform or venue restrictions before it escalates.

Operations:

- Develop victim-centered intake and reporting;
- Engage regularly with civil society organizations that already have community trust;
- Allow victims to have an advocate or representative in all interactions;
- Coordinated disruption of front groups and threat actors;
- Device forensics to check devices for spyware or other cyber intrusion capabilities.

News media and editors

Editorial safeguards:

- Verification protocols for potential smear dossiers;
- Secure source communications;
- Device hygiene for staff, freelancers, and fixers.

Coverage choices:

- Identify TNR as a public safety and rights issue;
- Expose threats and patterns, as well as incidents;
- Work with NGOs and civil society on incident coverage.

Protection and redress:

- Legal support for reporters under lawfare;
- Rapid flagging of platform abuse;
- Foster collaboration across newsrooms and NGOs, developing international partnerships on joint investigations and the sharing of safety guidance.

Parliamentarians, elected officials, public administrators, and diplomats

Lawmaking and oversight:

- Enact human-rights-compliant foreign-influence transparency registries for political activity with appropriate enforcement mechanisms;
- Enact and/or modernize anti-SLAPP legislation to protect victims, journalists, NGOs, etc., from retaliation and to provide support for defending against SLAPP suits;
- Ensure robust and consistent enforcement of sanctioned entities;
- Mandate annual public reporting on TNR incidents and outcomes while protecting victim and witness identities
- Regular briefings for elected officials and their staff on ongoing and emerging threats, and best practices to detect them;
- Ensure criminal codes cover TNR adequately such that investigations and prosecutions can be undertaken.

Budget, mandates, and procurement:

- Fund NGO reporting hotlines;
- Ensure law enforcement and government agencies tasked with threat monitoring and disruption are properly resourced;
- Ensure law enforcement is properly resourced to provide protection to victims and witnesses;
- Offer grants to NGOs and community groups that are working on building resilience against TNR;
- Exclude entities linked to TNR from public contracts.

Service delivery and protection:

- Provide multilingual reporting and support services;
- Expand legal aid and trauma-informed counseling;
- Limit data sharing with immigration agencies to protect victims and witnesses.

Constituency practice:

- Establish protocols for mitigating intimidation, secure meetings, evidence retention, and rapid referral to police and NGOs;
- Collaborate with trusted NGOs and other community actors to build trust with high-risk constituents;
- Deliver protective briefings to high-risk constituents.

Diplomacy and consular accountability:

- Create secure reporting channels through embassies;
- Use demarches and, when warranted, expulsion to address consular abuse;
- Coordinate allied visa bans and sanctions against perpetrators;
- Challenge abusive Interpol notices;
- Support at-risk activists with emergency documentation and referrals;
- Publish reports on recent transnational repression campaigns to increase transparency, strengthen strategic communication, and deter adversaries through concrete attribution;
- Strengthen targeted human rights sanctions and ensure robust and consistent enforcement.

FRAMEWORKS

This framework is designed for policymakers, law enforcement, civil society, community organizations and media to clarify the objectives, strategies, and tactics that foreign authoritarian regimes deploy in TNR operations. It is an operational primer and practical toolkit, intended to help readers anticipate, detect, disrupt, and respond to TNR across diplomatic, legal, digital, and physical domains.

FRAMEWORK STRUCTURE

The framework presents three high-level, broadly sequential stages of TNR activity:

Operation planning stages 11

Preliminary work to set political objectives, select targets, and design influence strategies.

Operation preperation changes..... 12

Actions to ready an operation, including target identification, surveillance, recruitment of assets, and technical preparatory work such as hacking or information engineering.

Operation execution stage 14

The suite of tactics used to carry out operations, from intimidation and defamation to legal harassment, kidnapping and, in extreme cases, assassination.

For each stage the framework lists likely tactics, techniques, and procedures adversaries may use, followed by practical countermeasures that governments, law enforcement, civil society, and vulnerable communities can deploy to preempt, disrupt, or deter those activities. Where useful, short illustrative examples from Russian and Chinese practices are provided to show how these methods have been applied in real cases.

HOW TO USE IT

Treat the framework as a living document. Use the stage checklists as diagnostic tools to map observed activity, select appropriate defensive measures, and coordinate responses across partners and jurisdictions. Prioritize victim safety, evidence preservation, and interagency information sharing.

The goal is to raise the operational cost for perpetrators, protect potential targets, and ensure robust assistance and accountability for victims.

1 OPERATION PLANNING STAGE

SETTING PRIMARY OBJECTIVES

- Defining desired political outcomes.
- Determining priorities.
- Developing strategies.
- Setting achievable objectives.
- Developing initiatives, such as policies, influence operations and broader transnational repression, and repatriation campaigns.

SETTING ACHIEVABLE OBJECTIVES

- **Develop narratives**
  Developing a positive or less critical image of the regime and activities abroad.

- **Manipulate public opinion**
  Developing information and influence campaigns
- **Undermine democracy and polarize target societies**
  Polarizing populations or inciting political conflict, including violence.

- **Suppress criticism**
  Disincentivizing criticism of regime activities—such as criticism of human rights violations and foreign interference.

- **Silencing regime critics**
  Using coercion and intimidation.

CHINESE EXAMPLES

"Telling China's stories well."

"The 'Fengqiao Experience' in the new era."

"Bringing consular service into the community."

RUSSIAN EXAMPLES

Undermining and destabilizing Western democracies.

Erosion of Western support for Ukraine and NATO unity.

Silencing critics of regime repression.

DEFENSIVE COUNTERMEASURES
Inoculation, deterrence, and threat reduction

- Establish a universal framework for collective response.
- Create a Global Alliance Against Transnational Repression (GAATR).
- Develop well-publicized tools to report suspicious activities and potential targeting within communities.
- Articulate existing consequences and clearly communicate that perpetrators face exposure, legal prosecution, visa bans, and asset freezes.
- Prepare law enforcement agencies to respond rapidly to new cases and provide support to victims.

IDENTIFYING TARGETS AND DEVELOPING TACTICS

- Reconnaissance and surveillance to identify targets that are susceptible to influence, intimidation/repression, or who are potential assets via online and offline means.

TTPs (TACTICS, TECHNIQUES, AND PROCEDURES)

- **Identifying potential regime aligned influencers**
  Monitoring social media for influencers who can act wittingly or unwittingly as amplifiers for regime information or influence operations, or in transnational repression operations. This includes those with pro-authoritarian, far-left, or far-right extremist sympathies.
- **Identifying regime critics**
  Monitoring media and social media accounts of officials, journalists, activists, organizations, and communities that are critical of the regime.
- **Organizing and co-opting diaspora groups and events**
  Organize cultural and social events to develop ties with diaspora communities, while conducting monitoring and surveillance under the guise of seemingly harmless "cultural" activities.

Physical surveillance

- Tracking movements and activities of targeted individuals.
- Monitoring attendance at events or gatherings.

Digital surveillance

- Monitoring social media profiles and online communications.
- Monitoring and identify polarizing issues to exploit during operations.
- Hacking personal devices and accounts.

CHINESE EXAMPLES

Organizing Chinese cultural events to identify potential targets for influence.

Identifying diaspora members who might be eligible to vote and may be susceptible to influence "pop-up" events.

Monitoring and executing operations using overseas police stations.

RUSSIAN EXAMPLES

Inviting susceptible academics, foreign officials, and journalists to participate in state think tanks and converting them to influencers.

Organizing cultural events to advance nationalist narratives and sentiment.

DEFENSIVE COUNTERMEASURES
Disruption, prevention, and deterrence

- Identify, warn, and provide support to potential targets.
- Expose and raise awareness of transnational repression tactics, techniques, and procedures.
- Enhance digital and operational security (OPSEC) and training for targeted individuals and groups.
- Establish an early warning system to identify and anticipate potential operations before they escalate.
- Preemptively expose regime-affiliated operations and issue timely warnings to the public and relevant officials.

2 OPERATION PREPARATION CHANGE

IDENTIFYING AND ESTABLISHING SOCIAL ASSETS

- Establishing information assets and ties with entities that can be leveraged for operations.
- Developing political assets that could potentially support the authoritarian regime's narratives and strategic agendas for exploitation or coercion.
- Strengthening ties with diaspora communities for political mobilization at a later stage.
- Practicing elite capture and strategic placement of agents.

TTPs (TACTICS, TECHNIQUES, AND PROCEDURES)

Creating regime-controlled organizations and think tanks

- Cultivating relationships with officials, policymakers, and academics, especially earlier in their careers, to develop long-term influence and advance regime interests under the guise of economic, social, and cultural cooperation.

Infiltrating diaspora communities

- Developing regime-aligned assets, placing informants within diaspora groups, and establishing front organizations to gather intelligence.
- Establishing information sharing, narrative amplification, and TNR strategies.

Developing assets targeting officials, politicians, and influencers

- Establishing relationships with identified former diplomats, officials, and politicians.
- Grooming and building of trust with targeted journalists.
- Developing relationships and information sharing with alternative media outlets.
- Enhancing existing relations with fringe far-left and far-right activists sympathetic to the regime.

CHINESE EXAMPLES

China Institute of Contemporary International Relations (CICIR), Chinese Academy of Social Sciences (CASS).

PRC flag-raising events in municipal spaces.

RUSSIAN EXAMPLES

Valdai Club, Russian International Affairs Council, Public Initiative "Creative Diplomacy" (PICREADI).

Regime-supported trade promotion agencies.

Global Research and Tenet Media.

Individuals who appear on and write for RT.

DEFENSIVE COUNTERMEASURES
Disruption, prevention, and deterrence

- Expose regime-controlled organizations, including:
  - think tanks and trade promotion organizations that often act as incubators for foreign influencers and proxies.
  - state-controlled and aligned media.
- Increase resources for law enforcement to detect, investigate, and disrupt and deter TNR behaviour.
- Support officials, researchers, activists, civil society organizations (CSOs) and community groups who are vulnerable to foreign influence campaigns.

MICROTARGETING

- Gathering information about the target.
- Analyzing the target background, personality, and social network via overt and covert means, including political affiliations, personal behaviors, past experience, financial status, and interpersonal relationships.
- Identifying vulnerabilities for exploitation.
- Determining specific strategies and tailored TTPs for the target (coercion, bribes or a combination).

TTPs (TACTICS, TECHNIQUES, AND PROCEDURES)

- **Tailoring strategies for different targets**
  Determining an execution plan.
- **Targeting civic institutions**
  Assessing the influence of potential targets based on their capacity to hinder advancement of regime interests or to expose regime criminality and operations.
- **Targeting influencers**
  Gathering of background information about targets to operationalize for future manipulation, including ethnic background and affiliations.

Surveillance and monitoring

- Conducting open source intelligence (OSINT) investigations on the target.
- Access To Information Request (ATIP) targeting government and academic related activities.
- Performing active surveillance of the target's public activities.

Spyware and online surveillance

- Phishing and hacking (with malware like Pegasus) to gain access to personal data and files.
- Planting incriminating evidence on personal devices for future exploitation.

CHINESE EXAMPLES

The three color-coded "political-interference tactics"

Blue: Cyber intrusion: Hacking devices and rooms to gather kompromat.

Gold: Financial influence: Bribes and covert payments.

Yellow: Sexual kompromat: Honey pots and other seduction tactics.

RUSSIAN EXAMPLES

Collecting and developing anti-Ukrainian narratives and monitoring of community, activists, and leaders.

Collect information in preparation to weaponize it against regime critics.

Invite potential assets to visit Russia and occupied regions of Ukraine.

DEFENSIVE COUNTERMEASURES
Disruption, prevention, and deterrence

- Raise awareness of foreign regime surveillance techniques and who could be targeted.
- Ensure vulnerable individuals and groups have access to tools and resources to counter digital campaigns, including malware and surveillance in the digital space.
- Ensure that law enforcement, officials, and media are aware of targeted groups and targeted individuals to prevent misunderstandings and potential false alarms.
- Ensure potential collaborators are aware of consequences.

2 OPERATION PREPARATION CHANGE

ESTABLISHING LEGITIMACY

- Developing and generating content and narratives that legitimize planned actions.
- Incorporating gray-zone activities and influence operations to further legitimize the attacker's assertiveness.

TTPs (TACTICS, TECHNIQUES, AND PROCEDURES)

Establishing legal content

- Leveraging existing laws and publishing guidelines for targeting certain individuals, groups, and organizations.
- Establishing domestic laws and legal frameworks to carry out transnational repression.

Creating preferred narratives

- Utilizing disinformation campaigns and influence operations to sow confusion and division.
- Creating and amplifying preferred narratives on social media to steer public opinion on the issues.

CHINESE EXAMPLES

National Security Law (2020) and Article 23 (2024).

Anti-Secession Law (2005) and the new judiciary guidelines on criminal punishment for Taiwan independence "separatists" (2024).

Creator narratives that frame the 2019 pro-democracy protest in Hong Kong as a "color revolution" and protesters as being manipulated by the United States and its allies.

RUSSIAN EXAMPLES

Criminalization of historical criticism of the Soviet regime, creating crimes against Russian history.

Criminalizing any diminishing of the "significance of the people's heroism in defending the Homeland is not permitted" (i.e., outlawing historical facts about Soviet crimes in Ukraine, Estonia, Latvia, and Lithuania).

Banning foreign criticism of the regime through foreign agents laws and designation of foreign critics and groups as "undesirable."

DEFENSIVE COUNTERMEASURES
Disruption, prevention, and deterrence

- Monitor and expose foreign narratives, and issue warnings.
- Monitor foreign legislative changes that might impact domestic activists and other potential targets.
- Share intelligence among democratic allies.
- Expose domestic amplifiers of foreign authoritarian narratives.
- Publicly reject politically motivated prosecutions of targeted individuals, and provide government support and visible solidarity with the victims.
- Coordinate with social media platforms to identify, flag and moderate false or defamatory narratives and the networks amplifying them.

MOBILIZING RESOURCES

- Mobilizing resources and coordinating different entities to execute influence operations and transnational repression campaigns.
- Mobilizing and activating both domestic and foreign agents to execute operations, including state security, intelligence, foreign agents, illegal agents, foreign assets, and influencers.

TTPs (TACTICS, TECHNIQUES, AND PROCEDURES)

Preparing and activating assets

- Inviting assets to visit perpetrator nations, including through conferences, travel junkets, and Ministry of Foreign Affairs meetings.
- Feeding state-developed narratives to assets via various platforms.
- Pitching disinformation and defamation to domestic journalists via diplomats.
- Raising regime issues within state-supported organizations—trade promotion, community, and issue-driven groups.
- Injecting narratives into identified far-left and far-right networks via social media, fringe media, and state media.
- Platforming regime-aligned assets on state media to legitimize and amplify messaging.

Establish and support state-aligned groups

- Activating regime-aligned trade promotion organizations to advance regime interests.
- Establishing astroturf groups to create the illusion of "grassroots" community representation.
- Supporting groups and events that promote anti-NATO, anti-Western, and anti-democratic positions.

CHINESE EXAMPLES

Coordination between Chinese state-affiliated entities and local Chinese organizations to implement the strategies.

Spamouflage campaign and the "50-cent army."

RUSSIAN EXAMPLES

Platforming of anti-government extremists on RT during Ottawa trucker occupation.

Embassy pitching anti-Ukrainian narratives to journalists.

Establishing astroturf Russian community group to lobby against Magnitsky sanctions.

Victory Day events.

DEFENSIVE COUNTERMEASURES
Disruption, prevention, and deterrence

- Expose regime-aligned groups.
- Actively enforce foreign influence transparency laws to ensure full compliance and deter covert operations.
- Reject municipal permits for regime-sponsored events when appropriate to local laws.
- Coordinated enforcement of sanctions laws to prevent collaboration with sanctioned entities and travel to sanctioned regions.
- Launch preemptive awareness campaigns ahead of significant events that foreign authoritarian regimes and their domestic proxies may seek to exploit or target.

3 OPERATION EXECUTION STAGE

DIGITAL TRANSNATIONAL REPRESSION: CYBER ATTACKS, DISINFORMATION, AND PROPAGANDA

- Exploiting digital vulnerabilities.
- Conducting influence operations to manipulate the information environment.
- Steering public opinion toward a favored direction.

TTPs (TACTICS, TECHNIQUES, AND PROCEDURES)

Hacking and data breaches

- Unauthorized access to personal, professional, or organizational networks.
- Denial-of-service-attacks (DDoS) on websites.

Malware and phishing

- Sending malicious links or attachments to compromise systems.
- Accessing and exploiting target contacts.
- Theft of data and sensitive documents.
- Planting of malicious surveillance software.

Disinformation and defamation campaign

- Planting fake news stories in media outlets.
- Promoting state narratives to undermine credibility.
- Creating fake profiles of targets to spread disinformation.

Platforms leveraged

- State media
- Social media
- Online forums
- Regime-aligned media
- Influencers

CHINESE EXAMPLES

APT 31, a hacking group run by China's Ministry of State Security (MSS), targeted Hong Kong pro-democracy activists in the United States and abroad.

RUSSIAN EXAMPLES

Russian agents' 2016 hacking of the US Democratic Party's server.

Chrystia Freeland disinformation campaign targeting her family.

Doppelganger campaign.

Ghostwriter campaign.

DEFENSIVE COUNTERMEASURES
Disruption, prevention, and deterrence

- Ensure robust, secure, and accessible reporting channels, backed by rapid and effective response mechanisms.
- Quickly and consistently investigate and prosecute both foreign and domestic violators when laws are violated.
- Regulate and limit availability of foreign influence platforms.
- Impose sanctions and initiate other diplomatic actions against foreign perpetrators for severe cases.
- Develop rapid-response mechanisms to support victims, including measures to mitigate digital, physical and psychological harm, and repair reputational damage and provide legal support.

HARASSMENT, INTIMIDATION AND COERCION

TTPs (TACTICS, TECHNIQUES, AND PROCEDURES)

Threatening communications and intimidation

- Threatening emails, messages, or phone calls.
- Anonymous or direct warnings to cease activities.
- Threats of sexual and physical violence.

Community intimidation

- Pressure by regime diplomats, proxies, and influencers to ostracize individuals.
- Economic isolation of targets.
- Intimidation and coercion of groups.

Pro-regime protests/event disruption

- Counter-protests organized by authoritarian diplomatic representatives to intimidate.

Defamation campaigns

- Spreading false information to discredit individuals.
- Public accusations of criminal or immoral behavior.
- Publishing of defamatory articles via state media influencers, or regime-aligned columnists.

Online harassment

- Coordinated trolling or cyberbullying.
- Doxxing personal information to the public.
- Campaigns to flood comments sections on traditional media and social media sites.
- Deep fake reports, images, and videos.
- Deploying influencers to attack targets.
- Use of community media, newspapers, radio, and online platforms to attack targets.

Blackmail

- Using compromising information to force compliance.
- Threatening to harm reputation or personal safety.

Harassment of family members

- Targeting relatives in the home country with threats, arbitrary detention, kidnapping, or legal actions.
- Using family as leverage to pressure individuals abroad.

CHINESE EXAMPLES

Harassment of families of overseas students.

Physical confrontations and intimidation during public demonstrations.

RUSSIAN EXAMPLES

Gender-based online violence.

Smear campaigns.

DEFENSIVE COUNTERMEASURES
Disruption, prevention, and deterrence

- Increase interoperability and maximize coordination between law enforcement, intelligence agencies, and foreign ministries, both domestically, and internationally among like-minded democratic governments to counter operations.
- Consistently prosecute all applicable criminal cases to the fullest extent of the law.
- Issue formal warnings to perpetrators engaging in sub-criminal threshold behaviour, making clear that escalating actions will trigger legal or diplomatic consequences.
- Expel diplomats and foreign nationals involved in hostile activities.

3 OPERATION EXECUTION STAGE

LEGAL AND JUDICIAL HARASSMENT "LAWFARE"

- Weaponizing legal systems to serve as a means of intimidation, coercion, and punishment.

TTPs (TACTICS, TECHNIQUES, AND PROCEDURES)

Sanctions, travel bans, visa coercion, and passport manipulation

- Application of sanctions on targets.
- Preventing individuals from entering or leaving certain countries.
- Forcing individuals to spy or promote regime propaganda at their destination in order to obtain visas.
- Refusing to renew passports or revoking citizenship.
- Denying consular services or legal assistance abroad.

Frivolous lawsuits

- Threatening lawsuits to intimidate targets.
- Filing baseless legal actions to burden individuals financially and psychologically.

Misusing and abusing of Interpol notices

- Issuing Red Notices based on fabricated charges.
- Attempting to extradite individuals through international law enforcement and Interpol.

Criminalizing individuals and issue bounties

- Criminalizing individuals in the name of "sedition," "colluding with foreign forces," or "threatening national security."
- Offering rewards (cash bounties) for information leading to the arrest of listed "fugitives."
- Freezing private property and assets.

CHINESE EXAMPLES

Establishment of the National Security Law (2020) and Article 23 (2024) criminalizing some activities of journalists, politicians, and protesters.

$1-million bounty placed on overseas pro-democracy activists.

Application of sanctions against twenty Canadians.

RUSSIAN EXAMPLES

Targeting of Kremlin critic Bill Browder with abuse of the Interpol Red Notice system.

Placement of hundreds of Canadians on Russian sanctions lists.

Threats of legal action against critics of the Russian government, and oligarchs to silence them.

DEFENSIVE COUNTERMEASURES
Disruption, prevention, and deterrence

- Target sanctions and diplomatic counter-measures in response to adversary-imposed sanctions and diplomatic pressure.
- Provide legal assistance for targets and victims of lawsuits.
- Coordinate with allies to prevent Red Notice abuse.
- Expose actors behind lawfare suits.
- Share information among allies about targets of foreign authoritarian sanctions to prevent travel delays.
- Protect and support citizens targeted by legal harassment.
- Condemn all forms of extradition initiated by perpetrator regimes.

PHYSICAL ATTACKS, VANDALISM, KIDNAPPING, ASSASSINATION

- Utilizing intelligence agencies, fronts, proxies, and local mobs or gangs to instigate violence against the target as a means to deter, coerce, retaliate, and intimidate through fear.
- Eliminating targets.

TTPs (TACTICS, TECHNIQUES, AND PROCEDURES)

Vandalism

- Vandalizing the target's property or community property intended to intimidate and provoke fear.

Kidnapping and unlawful detention

- Abducting individuals in foreign countries and returning them to their home country.
- Arresting individuals during international travel or in third countries.
- Collaborating with other states to detain and transfer individuals without due process.

Physical assault

- Conducting physical attacks intended to injure or intimidate.

Assassinations and poisoning

- Administering poison or other toxic substances to cause harm or death.
- Killing of targeted individuals abroad.

CHINESE EXAMPLES

"Operation Fox Hunt".

"Persuasion to Return" operations.

Kidnapping of Uyghur activist Hüseyincan Celil.

Vandalism of Hong Kong community pro-democracy businesses in Toronto.

RUSSIAN EXAMPLES

Poisoning of Alexander Litvenenko, Sergei Skripal, and others.

Vandalism of Ukrainian business, homes, and cars by radicalized extremists in Canada.

DEFENSIVE COUNTERMEASURES
Disruption, prevention, and deterrence

- Establish specialized law enforcement units trained to respond immediately to threats, vandalism, assaults, poisonings or suspicious incidents targeting high-risk individuals or communities.
- Monitor for early warning signs of plots, including surveillance and travel patterns, and share timely alerts with potential targets and law enforcement.
- Provide active threat monitoring, regular communication, and legal assistance to vulnerable individuals and groups.

CASE STUDIES

CASE STUDY

1. Canadian MP Michael Chong

Type of TNR: Influence operation and intimidation

Timeframe: May 4–13, 2023

Objectives: Discredit and intimidate

Actors/perpetrators: China

Operation entities: Chinese state media, state-affiliated accounts, and anonymous accounts

TTPs

Disinformation campaign

In August 2023, Global Affairs Canada's Rapid Response Mechanism announced that it had detected a Chinese information operation on WeChat targeting Member of Parliament (MP) Michael Chong.[19] Chong served as the foreign affairs lead for the Conservative Party, and has been an outspoken critic of China's treatment of its Muslim Uyghur population, and of the Chinese technology firm Huawei. The campaign coincided with diplomatic tensions between Canada and China, including the expulsion of a Chinese diplomat from Canada. It spread false narratives about Chong's identity—including commentary and claims about his background, political views, and family heritage—to discredit him among Chinese-speaking communities in Canada.

Surveillance and intimidation

Chong and his family were reportedly threatened and monitored in efforts to intimidate him.[20]

- A Chinese diplomat in Canada targeted Chong, seeking and collecting information about his relatives in Hong Kong to place sanctions on them and exert pressure on Chong through his family.
- According to the Canadian Security Intelligence Service and a report by the *Globe and Mail*, an intelligence officer from China's Ministry of State Security (MSS) took specific actions to target Canadian MPs. The officer gathered information about Chong and his family, which was likely transmitted back to the MSS.[21]

COUNTERMEASURES

Rapid Detection and Exposure of Disinformation

Deploy real-time monitoring of diaspora-targeted platforms like WeChat and rapidly publicize and debunk false narratives before they reach critical mass.

Protective Intelligence and Threat Alerts

Provide early warning to targeted officials about foreign collection of personal or family data, including actions by hostile diplomats.

Diplomatic Expulsion and Sanctions

Immediately expel diplomats engaged in intimidation or intelligence collection and apply targeted sanctions to implicated individuals and entities.

19. "Rapid Response Mechanism Canada Detects Information Operation Targeting Member of Parliament," Global Affairs Canada, August 9, 2023, https://www.canada.ca/en/global-affairs/news/2023/08/rapid-response-mechanism-canada-detects-information-operation-targeting-member-of-parliament.html.
20. Sarah Ritchie, "MP Michael Chong Decries 'Systemic Failure' to Notify Him of China's Alleged Threats," *CityNews*, May 16, 2023, https://toronto.citynews.ca/2023/05/16/june-byelections-monitored-foreign-interference-canada/.
21. Steven Chase and Robert Fife, "CSIS Head Tells MP Michael Chong that He and Family Were Targeted by China," *Globe and Mail*, May 2, 2023, https://www.theglobeandmail.com/politics/article-csis-confirms-mp-michael-chong-and-family-targeted-by-china/.

CASE STUDY

2. French MEP Raphaël Glucksmann

Type of TNR: Influence operation, online harassment, sanctions, lawfare, and diplomatic pressure

Timeframe: March 2021

Objectives: Discredit and intimidate

Actors/perpetrators: China

Operation entities: Chinese government, diplomats, and state-affiliated media

TTPs

Defamation and smear campaigns

- China accused Glucksmann of "maliciously spreading lies and disinformation" after the European Union (EU) imposed sanctions on Chinese officials and after he criticized China's mass human rights abuses against Uyghurs in Xinjiang.[22] The Chinese disinformation campaign targeting Glucksmann was aimed at discrediting his advocacy and undermining his political credibility.

Chinese state media and government officials labeled Glucksmann a "China basher" and claimed his actions were driven by ideological bias and anti-China sentiment.

- He was accused of spreading false information about the Uyghur conditions and supporting separatist movements.
- A China-aligned disinformation campaign accused Glucksmann "of being a Trojan horse for the Americans—particularly the [Central Intelligence Agency] in Europe" to discourage his advocacy on Chinese human rights issues.[23]

Online harassment

- Coordinated influence campaigns were deployed on social media, particularly targeting Glucksmann's posts about Uyghurs and Hong Kong.[24]
- Glucksmann received threats and derogatory messages from Chinese nationalists and bots.

Sanctions and diplomatic pressure

- In retaliation for EU sanctions against Chinese officials over human rights abuses in Xinjiang, China imposed sanctions on Glucksmann in March 2021.[25]
- Sanctions included travel bans to China, Hong Kong, and Macau, as well as the freezing of any assets he might hold in Chinese jurisdictions.

COUNTERMEASURES

Proactive Narrative Protection

Establish rapid-response fact-checking and counter-messaging to pre-empt and debunk state-led smear campaigns targeting elected officials.

Platform Collaboration Against Harassment

Work with social media companies to detect and report coordinated troll and bot networks, and state-sponsored harassment.

Protective Sanctions and Reciprocity

Implement reciprocal measures against foreign officials who impose politically motivated sanctions or engage in intimidation of elected representatives.

Public Solidarity and Institutional Backing

Ensure immediate public statements from national and EU institutions affirming the legitimacy of the target's work and rejecting foreign attempts to discredit or intimidate.

22. "China Hits Back at EU with Sanctions on 10 People, Four Entities over Xinjiang," Reuters, March 22, 2021, https://www.reuters.com/article/world/china-hits-back-at-eu-with-sanctions-on-10-people-four-entities-over-xinjiang-idUSKBN2BE1WB/.
23. "Raphael Glucksmann Ciblé par Une Campagne de Désinformation Pro-Chinois," *Challenges*, May 30, 2024, https://www.challenges.fr/politique/europeennes-glucksmann-averti-d-une-campagne-de-desinformation-le-visant_890382.
24. "Européennes: Glucksmann Averti d'Une Campagne de Désinformation le Visant, Provenant de Comptes Pro-Chinois," *Figaro*, April 16, 2024, https://www.lefigaro.fr/elections/europeennes/europeennes-glucksmann-averti-d-une-campagne-de-desinformation-le-visant-provenant-de-comptes-pro-chinois-20240416.
25. "Foreign Ministry Spokesperson Announces Sanctions on Relevant EU Entities and Personnel," Ministry of Foreign Affairs of the People's Republic of China, March 22, 2021, https://web.archive.org/web/20250418041611/https://www.mfa.gov.cn/eng/xw/fyrbt/fyrbt/202405/t20240530_11349690.html.

CASE STUDY

3. Former Estonian Prime Minister Kaja Kallas and her family

Type of TNR: Influence operation, online harassment, and surveillance

Timeframe: 2024

Objectives: Discredit, threaten, and intimidate

Actors/perpetrators: Russia

Operation entities: Russian government, intelligence, and state media

TTPs

Defamation and smear campaigns

- Prominent Estonian leaders and critics of the Kremlin have historically been significant targets of Russian malign information and influence operations. Kaja Kallas, Estonia's former prime minister who currently serves as high representative for foreign affairs and security policy and vice president of the European Commission, is an example of a targeted figure who will likely continue to be targeted by defamation and smear campaigns that aim to discredit, intimidate, and dehumanize her.
- Kremlin-aligned narratives have included false or exaggerated claims about her personal life or financial dealings, which were designed to undermine her reputation.[26]
- The Kremlin's "neo-Nazi" narrative has been aggressively deployed to discredit and dehumanize Kallas. In one instance, as part of the operation known as Portal Kombat or the Pravda Network, pro-Russia assets compared Kallas to Joachim von Ribbentrop, Adolf Hitler's minister of foreign affairs.[27]

COUNTERMEASURES

Proactive Narrative Protection

Establish rapid-response fact-checking and counter-messaging to preempt and debunk state-led smear campaigns targeting elected officials and the nations they represent.

Platform Collaboration Against Harassment

Work with social media companies to detect and report coordinated troll and bot networks, and state-sponsored harassment.

Legal and Diplomatic Pushback

Publicly reject politically motivated legal actions as illegitimate, and coordinate with EU and allied governments to impose appropriate punitive measures on perpetrators as permitted by law.

Protective Intelligence and Threat Alerts

Expand protective intelligence coverage to include online threat monitoring, open-source surveillance detection, and security support for the target's family, both domestically and abroad.

26. Marta Vunš and Kaili Malts, "PUUST JA PUNASEKS: Just Nii Käivitas Kreml Kaja Kallase Vastu Massiivse Valeinfokampaania," *Eesti Päevaleht,* July 4, 2024, https://epl.delfi.ee/artikkel/120305241/puust-ja-punaseks-just-nii-kaivitas-kreml-kaja-kallase-vastu-massiivse-valeinfokampaania.

27. "A Genetic Nazi and a True Aryan: Kaya Kallas Has Become Europe's New Ribbentrop," EuvsDisinfo, April 16, 2025, https://euvsdisinfo.eu/report/a-genetic-nazi-and-a-true-aryan-kaya-kallas-has-become-europes-new-ribbentrop/.

CASE STUDY (continued)

3. Former Estonian Prime Minister Kaja Kallas and her family

Online harassment and threats

- During her tenure as prime minister, Kallas was targeted by threatening and derogatory messages posted to social media platforms from accounts located outside of Estonia.[28]
- Troll farms and Kremlin-aligned accounts amplified accusations of Kallas being a "Russophobe" and a "Western puppet."[29]
- Kremlin-aligned influencers made threats against Kallas and her family, including anonymous messages suggesting violence.[30]

Intimidation

- The Estonian Internal Security Service said in its 2024–2025 annual report that the Russian Investigative Committee publicly announced charges against Kallas in absentia.[31] This was likely an effort to discredit Kallas and disqualify her for any future international postings, such as her current roles as high representative for foreign affairs and security policy and vice president of the European Commission.

28. Tarmo Jüristo, "Perhaps We're Not About to Get Used to Threats," *ERR News*, November 26, 2019, https://news.err.ee/1006857/tarmo-juristo-perhaps-we-re-not-about-to-get-used-to-threats.
29. Kaili Malts, "Disinformation Landscape in Estonia," EU DisinfoLab, January 10, 2025, https://www.disinfo.eu/wp-content/uploads/2025/01/20250110_Disinfo-landscape-in-Estonia.pdf; "Queen of Russophobia: History of Top EU Diplomat's Blatant Anti-Russian Stance," RT, February 5, 2024, https://archive.is/0DDWy.
30. Karel Reisenbuk, "Account behind Kallas Threat Exclusively Pro-EKRE," *Postimees*, November 18, 2019, https://news.postimees.ee/6828804/account-behind-kallas-threat-exclusively-pro-ekre.
31. "Annual Review 2024–2025," Estonian Internal Security Service, 2025, https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf.

CASE STUDY

4. Former Latvian Defence Minister Artis Pabriks

Type of TNR: Influence operation, cyberattacks, and online harassment

Timeframe: 2015–present

Objectives: Discredit and intimidate

Actors/perpetrators: Russia Operation entities: Russian government, intelligence, and state media

TTPs

Disinformation campaign

- Artis Pabriks is a prominent former Latvian minister of defense and foreign affairs, and a vocal critic of the Kremlin. He has been targeted by fabricated stories and narratives aimed at undermining his credibility both inside Latvia and among Latvia's NATO allies (including Canada, which leads NATO's enhanced Forward Presence in Latvia). As the Kremlin often does, it has published and amplified narratives that manipulated and exaggerated historical facts to suggest Pabriks supports neo-Nazis (the same narrative used against Kallas and Ukrainian President Volodymyr Zelenskyy).[32]

Intimidation and sanctions

- In the wake of Russia's illegal annexation of Crimea, Pabriks was placed on Russia's blacklist in 2015, banning him from entering Russia. This move was likely intended to intimidate and discredit Pabriks internationally and within Latvia.[33]

Cyberattacks

- As part of a reported phishing attack, Russian-backed groups targeted Pabriks's communications and the Ministry of Defense during his tenure.[34]
- In February 2019, according to the Latvian Ministry of Defense, numerous email accounts in Latvia received a message containing false and damaging information that was allegedly signed by then Defense Minister Pabriks. The emails were sent from servers based in Russia and contained a message about Pabriks spending time in Riga bars and engaging in indecent activities. The emails might have been part of a phishing campaign and an effort to discredit Pabriks.

COUNTERMEASURES

Advanced Cyber Defence and Threat Hunting

Implement continuous phishing detection, penetration testing, and advanced email authentication (SPF, DKIM, DMARC) to block spoofed or falsified messages.

Real-Time Disinformation Monitoring and Rapid Rebuttal

Track state-linked media and social channels for emerging smear narratives, and deploy factual counter-messaging through trusted Latvian, NATO, and allied channels before false claims spread.

Platform Collaboration Against Harassment

Work with social media companies to detect and report coordinated troll and bot networks, and state-sponsored harassment.

Public Solidarity and Institutional Backing

Ensure immediate public statements from national and EU institutions affirming the legitimacy of the target's work and rejecting foreign attempts to discredit or intimidate.

32. "Latvian Waffen-SS Legion 'Pride of Our State and Nation,' Defense Minister Says, as He Honors WW2 Veterans Who Sided with Hitler," RT, September 28, 2019, https://web.archive.org/web/20241026125809/https://www.rt.com/news/469852-latvia-legion-veterans-pride/.
33. "EU Criticises Russia's Blacklist, Where 20 of 89 Persons Included Are from Baltics," Baltic News Network, June 1, 2015, https://bnn-news.com/eu-criticises-russias-blacklist-20-89-persons-included-baltics-129699.
34. "Latvian State Institutions and Politicians Experience Cyber Attack," Latvian Public Media, December 13, 2019, https://eng.lsm.lv/article/society/defense/latvian-state-institutions-and-politicians-experience-cyber-attack.a341632/.

CASE STUDY

5. Inter-Parliamentary Alliance on China (IPAC)

Type of TNR: Cyberattacks

Timeframe: Approximately 2021

Objectives: Hacking, surveillance, and maligning reputation

Actors/perpetrators: China Operation entities: MSS intelligence officers, contractor hackers, and support personnel

The targets included EU and UK members of IPAC who had been outspoken on topics relating to the Chinese government.

TTPs

Cyberattack by Advanced Persistent Threat (APT 31)

- In or about January 2021, the conspirators registered and used ten conspirator-created accounts on an identified mass email and mail merge system to send more than one thousand emails to more than four hundred unique accounts of individuals associated with IPAC. The mailing tool used in this campaign enabled the conspirators to track delivery metrics on emails and receive data from victims that opened the nine emails, including the victims' Internet Protocol (IP) addresses, browser types, and operating systems.

COUNTERMEASURES

Advanced Cyber Defence and Threat Hunting

Implement continuous phishing detection, penetration testing, and advanced email authentication to block spoofed or falsified messages.

Threat Intelligence Sharing and Alerts

Establish real-time information-sharing channels between organization members, national cybersecurity agencies, and allied governments to flag APT activity and suspicious infrastructure early.

Regular Cybersecurity Training

Provide ongoing phishing simulation exercises and security awareness training for parliamentarians, staff, and affiliated organizations to reduce the risk of compromise.

CASE STUDY

6. Chrystia Freeland and the Ukrainian Canadian community

Type of TNR: Influence operations, sanctions, and disinformation

Timeframe: 2014–present

Objectives: Discredit and intimidate

Actors/perpetrators: Russia Operation entities: Russian intelligence, Ministry of Foreign Affairs, state media, domestic proxies, and influencers

TTPs

Defamation campaigns and influence operations

- Since the Cold War, Moscow has consistently used disinformation tactics to delegitimize its critics by branding them as "fascists" or "Nazis."
- These disinformation tactics have been weaponized against prominent Central and Eastern European figures, community leaders, activists, and the broader Ukrainian-Canadian community.
- Chrystia Freeland—Canada's Special Envoy to Ukraine and former minister of transport, foreign affairs, deputy prime minister, and minister of finance—was targeted for her outspoken criticism of the Kremlin and her support for Magnitsky Act-style sanctions in Canada.
- In early 2017, a pro-Kremlin blog based in Moscow amplified false allegations that Freeland's grandfather collaborated with Nazi forces in Western Ukraine during World War II.
- These claims were further amplified by the Russian embassy in Ottawa and pitched to Canadian media, framing Freeland as someone who "whitewashed" her grandfather's past and supported "neo-Nazism."[35]
- Two prominent Canadian newspapers reported elements of the story.[36]
- This false narrative continues to circulate within Canada's extreme far-left and far-right information ecosystems.

COUNTERMEASURES

Proactive Narrative Protection

Establish rapid-response fact-checking and counter-messaging to preempt and debunk state-led smear campaigns targeting elected officials and the nations they represent.

Media Resilience and Journalist Training

Provide Canadian journalists and editors with training and resources to recognise and avoid amplifying foreign disinformation, including guidance on how to verify politically motivated historical claims.

Platform Collaboration Against Harassment

Work with social media companies to detect and report coordinated troll and bot networks, and state-sponsored harassment.

Support for At-Risk Communities

Offer secure reporting channels, law enforcement liaison programs, and protective measures for vulnerable communities, institutions, events, and leaders facing threats or vandalism.

Public Condemnation and Sanctions Reciprocity

Publicly denounce politically motivated foreign sanctions against Canadian officials or communities, and apply reciprocal measures to foreign officials, expulsion of agents and diplomats, and condemning of proxies involved in such operations.

35. Justin Ling, "My Dinner With Kirill," *Bug-eyed and Shameless* (blog), March 24, 2023, accessed June 19, 2025, https://www.bugeyedandshameless.com/p/my-dinner-with-kirill.

36. Terry Glavin, "How the Russians Tried to Smear Chrystia Freeland," *Ottawa Citizen*, March 8, 2017, accessed June 18, 2025, https://ottawacitizen.com/opinion/columnists/glavin-how-the-russians-tried-to-smear-chrystia-freeland.; Marcus Kolga, "Stemming the Virus: Understanding and Responding to the Threat of Russian Disinformation," *Macdonald–Laurier Institute*, December 11, 2018, accessed June 18, 2025, https://macdonaldlaurier.ca/files/pdf/20181211_MLI_Russian_Disinformation%20PAPER_FWeb.pdf.

CASE STUDY (continued)

6. Chrystia Freeland and the Ukrainian Canadian community

Physical harassment and violence

- The Kremlin's ongoing dehumanization of Ukrainians and diaspora Ukrainians has incited hate, contributing to a noticeable rise in anti-Ukrainian incidents.
- Members of the Ukrainian community have reported acts of vandalism across Canada.
- A prominent Ukrainian-Canadian-owned bakery in Toronto was defaced with Russian nationalist and anti-Ukrainian graffiti.[37]
- Ukrainian students at the University of Ottawa have reported increased harassment and intimidation.[38]

Sanctions and intimidation

- Following the full-scale invasion of Ukraine in 2022, the Kremlin issued retaliatory sanctions against prominent Canadians critical of Russian aggression, including leaders within the Ukrainian-Canadian community.
- The timing and substance of these sanctions underscore Moscow's strategy to intimidate, discredit, and silence critics and diaspora voices who advocate for Ukraine and counter Russian disinformation.
- The publication of these sanctions also serves to signal potential targets to ideologically aligned proxies and influencers, encouraging further defamation and harassment.

37. Catherine McDonald, "Ukrainian Bakery in Toronto Vandalized Again," *Global News*, March 4, 2022, https://globalnews.ca/news/8659644/ukrainian-bakery-toronto-vandalized-again/.
38. Ben Andrews, "Anti-Ukrainian Hate Symbols, Harassment at University Campuses," CBC News, February 22, 2023, https://www.cbc.ca/news/canada/ottawa/anti-ukrainian-hate-symbols-harassment-university-campuses-1.6733813.

Conclusion

Foreign interference and transnational repression rarely occur in broad daylight. They thrive in the shadows—exploiting the legal, ethical, and institutional blind spots of liberal democracies. Yet this ambiguity does not leave democracies powerless. There are critical countermeasures that can and must be deployed to defend the integrity of institutions and protect the individuals and communities most at risk. These tools—legally grounded, innovative, and adaptable—must be designed not only to blunt the immediate impact of coercive tactics but to deter authoritarian regimes from ever considering democracies as susceptible to their campaigns of fear and control.

While the case studies in this report all discuss actions perpetrated by Russia and China, it is essential to note that these two countries are not the sole actors involved in this global phenomenon. Many countries worldwide are also engaged in TNR, with data covering incidents perpetrated by forty-eight governments between 2014 and 2024.[39] Beyond Russia and China, other major perpetrators implicated in TNR in the past decade include Iran, Saudi Arabia, Turkey, North Korea, Egypt, Cuba, Cambodia, Rwanda, Belarus, and Venezuela.

These governments have launched attacks against exiles and members of the diaspora, using a combination of digital and physical assaults. These can include digital surveillance and online defamation to support arbitrary detentions, abductions, and assassinations. The authors look forward to developing case studies and further documenting cases linked to these additional repressive states to enhance understanding of transnational authoritarian practices.

At the heart of this framework is a clear objective: to establish a universal model that identifies the indicators and TTPs associated with FI and TNR, and to outline concrete, scalable countermeasures that can be implemented at each stage of an operation. This approach requires not just coordination across government departments but a sustained, collective response among like-minded democratic allies.

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

Recommendations

- Develop and deploy an early warning system supported by a shared, cross-national database and regular threat analysis that integrates human intelligence (HUMINT), signals intelligence (SIGINT), and open-source intelligence (OSINT). This will strengthen both interoperability and response speed.
- Make unclassified intelligence—especially OSINT—accessible to the public (while protecting victim and witness personal information) to enhance strategic communication, build public resilience, and expose malign actors.
- Institutionalize collaboration with civil society. Researchers, journalists, academics, and human rights organizations are not bystanders; they are frontline defenders and invaluable partners in exposing and countering authoritarian threats.
- Expose instances of TNR when in the public interest. This will help to discredit false narratives and impose costs on perpetrators.
- Provide adequate resources and frameworks to protect victims and witnesses.

Because these threats are systemic and orchestrated by hostile authoritarian regimes, the response must be equally systemic. A whole-of-society strategy—one that bridges national, provincial, and municipal levels of government and leverages the expertise and networks of civil society and affected communities—is the only effective way to preserve the democratic values that these operations seek to erode.

Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council
1400 L Street NW, 11th Floor
Washington, DC 20005

(202) 463-7226

www.AtlanticCouncil.org