POLICY PAPER

Terrorist Threats to Canada

Originating in Central Asia, Middle East, Afghanistan and Pakistan

Faramarz Tamanna
Centre for International Policy Studies (CIPS),
University of Ottawa, Nov. 2026



Université d'Ottawa
CÉPI
Centre d'études
EN POLITIQUES
INTERNATIONALES

University of Ottawa
CIPS
Centre for
INTERNATIONAL
POLICY STUDIES

--------- CIPS POLICY PAPER ---------

Terrorist Threats to Canada

Originating in

Central Asia, Middle East, Afghanistan and Pakistan

Faramarz Tamanna

CIPS, University of Ottawa

Nov. 2026

The Author



Faramarz Tamanna is a Research Associate (since 2023) at the Centre for International Policy Studies (CIPS) and Visiting Professor (2025), Graduate School of Public and International Affairs (GSPIA), University of Ottawa, and a Part-time Professor at the School of Conflict Studies and the School of Ethics and Public Affairs, Saint Paul University. He was a Postdoctoral Fellow at GSPIA (2024–2026).

His research examines security and conflict in Afghanistan, Pakistan, Iran and Central Asia; terrorism; defence; external intervention, statebuilding and political settlements; and the foreign policy and geoeconomics of regional order.

Before joining CIPS, Dr. Tamanna was Professor at the School of Diplomacy and International Studies, University of Afghanistan (2012–2023), and Director General of the Centre for Strategic Studies at Afghanistan's Ministry of Foreign Affairs (2012–2018), where he led the senior team that drafted Afghanistan's Foreign Policy. From 2013 to 2018 he also taught the Ministry of National Defence's strategic course for senior intelligence and military officers.

He holds a PhD in International Studies from Jawaharlal Nehru University, New Delhi (2014), and an MA in International Relations (2006) and a BA in Political Science (2001) from Shahid Beheshti University, Tehran. He has taught at universities in Afghanistan since 2008 and in Canada since 2024.

He is the author of four books and the editor of a fifth: *Afghanistan's Foreign Policy: Dynamism, Scope, Actions* (University of Afghanistan, 2021); *The Dilemma of Peace and Security in Afghanistan* (University of Afghanistan, 2020); *Political Development in Afghanistan* (Amiri, 2019); *US Foreign Policy in Afghanistan* (Research Institute of Strategic Studies, Tehran, 2008); and, as editor, *Afghanistan's Foreign Policy: On Regional Cooperation* (Ministry of Foreign Affairs, Kabul, 2014). He has also published journal articles, book chapters and policy papers on international relations, foreign policy and security.

Email: fz.tamanna@gmail.com

Terminology and Classification

The identification and classification of organizations discussed in this paper are based on publicly available official Canadian government documents, including the Government of Canada's list of terrorist entities under the Criminal Code and relevant publications of Canadian security and intelligence agencies. References to organizations as "terrorist" reflect their official designation by Canadian authorities where applicable, rather than an independent legal determination by the author. This paper is an independent academic and policy analysis intended solely to examine potential security implications for Canada. It does not advocate for or against any organization, political movement, or religious community.

List of Acronyms and Abbreviations

AQAP — Al Qaida in the Arabian Peninsula
AQIS — Al Qaida in the Indian Subcontinent
BLA — Balochistan Liberation Army
CBSA — Canada Border Services Agency
CSE — Communications Security Establishment
CSIS — Canadian Security Intelligence Service
DND — Department of National Defence
ETIM — Eastern Turkistan Islamic Movement
FATF — Financial Action Task Force
FINTRAC— Financial Transactions and Reports Analysis Centre of Canada
G7 — Group of Seven
GAC — Global Affairs Canada
IMU — Islamic Movement of Uzbekistan
IRCC — Immigration, Refugees and Citizenship Canada
IRGC — Islamic Revolutionary Guard Corps
ISKP — Islamic State Khorasan Province
ITAC — Integrated Terrorism Assessment Centre
NATO — North Atlantic Treaty Organization
NORAD— North American Aerospace Defense Command
NSIA — National Security and Intelligence Advisor
PCO — Privy Council Office
RCMP — Royal Canadian Mounted Police
TIP — Turkistan Islamic Party
TTP — Tehrik-e-Taliban Pakistan
UN — United Nations
US — United States

Table of Contents

Executive Summary 1

What this Paper Proposes 3

Methodology and Theoretical Framing 4

Theoretical and Policy Contribution: A Canadian Model of Networked Counter-Terrorism Self-Reliance 5

Strategic Logic and Analytical Framework 7

Threat Map: Afghanistan, Pakistan, Central Asia and the Middle East 11

A Balanced Assessment: What the Data Does Not Support 12

Linking Threats to Canada's National Interests 13

Canadian Evidence of the Threat 15

Existing Gaps in Canadian Policy 16

Proposed Framework and Practical Recommendations 18

Conclusion 22

References 24

Executive Summary

Canada should move from a reactive and listing-centred counter-terrorism posture to a network-centred, interests-centred and resilience-centred one, making the Canadian Threat-to-National Interest Transmission Matrix, updated every 90 days by an interdepartmental mechanism, the basis for decisions on listing, sanctions, intelligence resources and prevention programming. Seven pillars follow. The first move is Pillar Two, reform of the authorization regime for activities in geographic areas controlled by a terrorist group: no new legal authority, no prerequisite, the lowest cost of the seven, and it can begin immediately (Public Safety Canada, 2025e). The locus of danger for Canada is no longer groups based in a single geography but interconnected ecosystems. "Ecosystem" here means geographic proximity, a shared safe haven, common flows of fighters and money, and shared propaganda and financial infrastructure; it does not mean unified command or centralized operational coordination.

What has not changed is the threat level. Canada's National Terrorism Threat Level remains MEDIUM, an attack is assessed to be a realistic possibility and has not changed since 2014 (Government of Canada, 2025). The argument here rests on a change in the mix of transmission pathways, not on an increase in the intensity of the threat. The regional evidence, a facilitating environment in Afghanistan, and ISKP retaining strong capability and the intent to conduct external operations, establishes that Canada is not exempt; it does not establish that Canada is specifically targeted (United Nations Security Council, 2026).

Three transmission pathways are documented in Canada: *Online recruitment of young people.* Close to one in ten CSIS terrorism investigations involves at least one person under eighteen; five minors were arrested in 2023, two in 2024 and four in 2025. At least seven priority mobilization-to-violence investigations were assessed as wholly or partly influenced by the Middle East war (CSIS, 2026).

Organizational connection at the level of criminal cases. Two returned Canadian extremist travellers were convicted in 2025 of participating in the activities of a terrorist group (CSIS, 2026);

in the July 2024 Greater Toronto Area case two accused were prosecuted for conspiracy to commit murder on behalf of the Islamic State (Public Safety Canada, 2024).

State transnational repression. CSIS describes Iran as an aggressive perpetrator; after several Iranian plots were disrupted, Canada and thirteen other countries issued a joint statement in July 2025 (CSIS, 2026). This is the most fully realized pathway documented in the paper.

The evidence does not establish the magnitude of these pathways or their primacy over other threats. Where direct Canadian evidence is absent, shipping disruption's economic effect, the link between Central Asian networks and domestic security, the claim is a potential pathway, not a measured effect.

The most important negative finding runs against this paper's own geography: CSIS assesses that youth radicalization in Canada concentrates mainly in online neo-Nazi and nihilistic violent extremism ecosystems (CSIS, 2026). That supports the pathway-centred model rather than undermining it: if the pathway rather than the geography is the unit of analysis, adolescent online recruitment is one pathway whatever its ideological origin, intervention should follow the mechanism, not the ideology.

Canada's national counter-terrorism strategy, Building Resilience Against Terrorism, dates from 2012 and still guides more than twenty federal departments and agencies (Public Safety Canada, 2012); the National Strategy on Countering Radicalization to Violence dates from 2018 (Public Safety Canada, 2018). Those documents predate the rise and fall of the Islamic State caliphate, the Taliban's return in 2021, ISKP as an external-operations actor, adolescent online radicalization in its present form, crypto-asset-based financing, and transnational repression as an independent policy agenda. Four gaps follow.

First, listing logic dominates network analysis. The 2024 and 2025 listings, the IRGC, Ansarallah, four further entities in December 2025, do not reach networks operating through media, logistics, financial intermediaries and commercial covers (Public Safety Canada, 2025b).

Second, counter-terrorism policy is separated from assistance and field presence. The authorization regime is treated as an instrument of legal and humanitarian compliance rather than a strategic one (Public Safety Canada, 2025e).

Third, diaspora protection is fragmented across the RCMP, CSIS, GAC, IRCC and local institutions, which makes victim reporting difficult and yields no single picture of risk; the Countering Foreign Interference Act covers democratic-process interference, not the operational protection of individuals targeted by transnational repression (Parliament of Canada, 2024).

Fourth, dependence on American intelligence and operational leadership remains excessive, under 2025–2026 US pressure on Canada's defence share (Public Safety Canada, 2025c; Reuters, 2026b).

What this Paper Proposes

Pillars One and Five answer the first gap, Pillar Two the second, Pillar Three the third, Pillars Four and Seven the fourth; Pillar Six is cross-cutting.

Pillar One. A South and Central Asia–Middle East joint analytical cell under PCO/NSIA, with GAC, CSIS, RCMP, FINTRAC, CBSA and CSE, mandated to integrate threat data and not only collect it; within it, the Canada Khorasan–Levant Early Warning Hub.

Pillar Two. Conversion of the authorization regime into a strategic instrument: a faster, more transparent and mandate-driven pathway for accredited Canadian organizations on the Afghanistan and Syria files.

Pillar Three. A National Protocol for the Protection of Communities Exposed to Transnational Repression and Cross-border Extremism, and the Diaspora Protection and Partnership Compact, inclusion by exposure to threat, not ethnic or national belonging.

Pillar Four. Diversified security diplomacy with non-US allies: a multi-domain counter-terrorism minilateral, the United Kingdom first, then Australia, New Zealand and Japan.

Pillar Five. Targeting the infrastructure that supports terrorism, not armed cores alone, media, crypto-assets, logistical intermediaries, commercial covers, propaganda circles, through listing, sanctions, financial monitoring and law enforcement.

Pillar Six. Legal-policy differentiation among groups on four criteria, intent to conduct external operations, capability, an access pathway to Canada, capacity for domino effects, with an operationally integrated response.

Pillar Seven. Linking counter-terrorism to continental defence doctrine and national resilience, ports and airports, energy and telecommunications infrastructure, combined terrorism/cyber exercises.

Pillar Two first. In the first six months: the joint analytical cell, the threat classification matrix, and reform of the authorization regime process. At twelve months: a pilot of the diaspora protection protocol and design of the minilateral. At eighteen to twenty-four months: linking these outputs to decisions on listing, targeted sanctions, critical-infrastructure protection, and Canada's diplomatic and development presence in high-risk environments.

Two components are conditional on legal determination and should not enter implementation before it: the Canada Khorasan–Levant Early Warning Hub, and the policing component of the diaspora protocol. The Compact is the costliest and most sensitive recommendation; it should proceed as a limited pilot, evaluated independently before expansion. The real test is whether counter-terrorism policy purchases security at the cost of trust or builds it upon trust.

Methodology and Theoretical Framing

This text is an open-source-based policy paper, and its documentation has three layers. The first layer consists of official Government of Canada documents: the list of terrorist entities, the public report of the Canadian Security Intelligence Service (CSIS), the departmental plan of Global Affairs Canada, the transition documents of Public Safety Canada, and reports concerning the authorization regime for activities in geographic areas controlled by a terrorist group. The second layer consists of the reports of the UN Security Council Analytical Support and Sanctions Monitoring Team. The third layer consists of the indices of research institutes and reports from reputable news agencies for current events. The author had no access to classified assessments; accordingly, no data from closed or classified sources have been used in this text.

The selection of actors capable of posing a threat to Canada's national interests rested on three criteria: first, the actor's presence in the assessment of the UN Monitoring Team as an active player in the geography with which this policy paper is concerned; second, the existence of at least one durable pathway connecting it to one of Canada's stated national interests; third, policy relevance for Canada, whether by legal status on the list of terrorist entities or by importance to Canada's security partners.[1]

Theoretically, the framework of this policy paper rests on four bodies of existing literature. This text does not claim to replace any of these literatures, and its claim to novelty is limited and specific:

First, the literature on the network analysis of terrorism. Perliger and Pedahzur argue that the move from the analysis of the "organization" to the analysis of the "network" makes it possible to understand dynamics of recruitment, structure and operational capacity that organization-centred approaches miss (Perliger & Pedahzur, 2011). This policy paper accepts that insight but shifts the unit of analysis: from the group's internal network to the pathway connecting the group to the national interests of a third state. In other words, what is seen here as a network is not merely the actor's structure but the set of channels through which risk is transmitted.

Second, the literature on hedging strategy in middle and small states. Kuik defines this strategy as "insurance-seeking behavior under situations of high uncertainty and high stakes" and shows that weaker states, instead of choosing between balancing and bandwagoning, employ a combination of both in order to preserve strategic flexibility (Kuik, 2016, 2021). The concept of "networked security self-reliance" in this text is a form of that same logic, applied to the counter-terrorism domain: not a rupture with the existing security umbrella, but the construction of alternative capacity in those areas where dependence carries the costliest consequences.

[1] Actors that met only the third criterion, such as the BLA, are discussed with an explicit statement of their legal status.

Third, the critical literature on community-based programs for countering extremism. In their study of the experience of the United Kingdom's Prevent programme, O'Toole and colleagues show that the program was not a coherent disciplinary project but a field of dispersed implementation, of conflict between security institutions and social cohesion institutions, and of resistance and redefinition by Muslim communities themselves; at the same time they state explicitly that the underlying logic of Prevent has been "deeply problematic" for the relationship between the state and Muslim communities (O'Toole et al., 2016). This finding carries two direct lessons for the design of the diaspora protection compact in this document: first, that declaring a commitment to non-securitization is not sufficient and that institutional design must guarantee it; second, that a referral mechanism, if it is not accompanied by community trust, leads to a decrease in reporting rather than an increase. For that reason, the criterion of inclusion in the compact proposed in this document is defined as "being exposed to a threat" and not as ethnic or national belonging.

Fourth, the literature on "threat inflation". Thrall and Cramer have shown that security documents are prone to threat inflation and to institutional inferences that go beyond the evidence (Thrall & Cramer, 2009). This policy paper has consciously taken a position against such a danger: Canada's unchanged threat level is stated explicitly in the Executive Summary; disconfirming findings are presented in the section "A Balanced Assessment"; and transmission claims, where Canadian evidence does not exist, are explicitly called a "potential pathway" and not "actual transmission".

Theoretical and Policy Contribution: A Canadian Model of Networked Counter-Terrorism Self-Reliance

The principal contribution of this policy paper is that it analyzes terrorism not merely as a threat from armed groups but as a network of pathways transmitting risk to Canada's national interests. In a considerable part of listing practice and of the prevailing policy literature in Canada, the main focus is on the names of groups, their ideology, or their legal status on terrorist lists. This text, while accepting the importance of listing, argues that such an approach is not sufficient for Canada's security environment and for the requirements of international security in 2026 and beyond. Threats arising from Afghanistan, Pakistan, Central Asia and the Middle East are today transmitted to Canada through financial, digital, cyber, diaspora, diplomatic, geopolitical, migration and supply-chain pathways. The central question is therefore not only "which terrorist group is active?" but "which group, through which pathway, threatens which Canadian national interest?"

On this basis, this policy paper proposes a model for examining the "threat-to-national-interest" transmission pathway. The model links three levels of analysis: first, the level of threat actors; second, the level of transmission pathways; and third, the level of Canada's national interests, comprising the security of citizens, social cohesion, economic security, critical infrastructure, the

credibility of alliances and independence of strategic decision-making. “Transmission pathway” in this document means any specific mechanism through which the capability or intent of a threatening actor could harm one of Canada’s national interests. These pathways are not equal in their demonstrability: some, such as a financial transaction or a cyber attack, are observable and attributable events, while others, such as “inspiration”, are ideational effects for which there is no agreed attribution mechanism. This document takes that distinction into account in its interpretation. This framework allows Canada to prioritize threats not in a scattered fashion but based on their direct relation to national interests.

The second contribution of this document is the proposal of the concept of “networked security self-reliance”. In positive terms, the concept consists of Canada’s capacity to maintain independent analysis, language coverage, financial and cyber capacity and regional knowledge at a level that would allow it to continue making independent decisions even in the absence or reduction of support from a single partner. In negative terms, the concept does not mean severing cooperation with the United States, NATO or the Five Eyes; it means reducing Canada’s vulnerability to excessive dependence on a single security umbrella. Canada should maintain its traditional cooperation with the United States while at the same time strengthening its independent analytical, linguistic, financial, cyber, diplomatic and regional-expertise capacity. In such a model, the United Kingdom, Australia, New Zealand, the European Union, France, Germany, Japan and selected regional partners can form the second layer of Canada’s security resilience. The objective is not the immediate replacement of the United States; the objective is to build strategic room for manoeuvre for Canada.

The third contribution is a redefinition of the place of the diaspora in Canada’s counter-terrorism policy. This document emphasizes that Afghan, Pakistani, Iranian, Arab, Kurdish, Tajik, Uzbek and other communities connected to these regions must not be seen as objects of collective suspicion. In many cases they are the victims of threat, intimidation, extortion, extremist propaganda, transnational repression and pressure from foreign networks. Effective counter-terrorism policy must therefore define them as partners in protection, early warning, social resilience and regional knowledge. It should be added that the “diaspora” in this document is not a homogeneous population: an activist who is the target of a state’s transnational repression and a family worried about the radicalization of its teenager are two different situations requiring two different kinds of intervention; policy design must reflect that difference.

The value added by this policy paper lies in converting a theoretical concept into an operational instrument: from the “Threat-to-National Interest Transmission Matrix” to the “Khorasan–Levant Early Warning Hub”, and from the “Diaspora Protection and Partnership Compact” to “counter-terrorism minilateral cooperation with non-US allies”. In that sense, the present document is not merely a security review; it is an attempt to design a Canadian, realistic, rights-based and forward-looking architecture for countering terrorism in a period when the boundary between external threat and internal vulnerability has become more fluid than at any other time.

Strategic Logic and Analytical Framework

At the outset, the framework of "Canada's national interests" is determined based on this country's official documents, not on the basis of the mere listing of terrorist groups. This document does not claim to offer a theoretical definition of the national interest; rather, it uses the Government of Canada's own stated framework as the operational basis for prioritization. According to the Global Affairs Canada departmental plan for 2025–2026, the Government of Canada defines its interests in connection with the security and well-being of Canadians, the resilience of supply chains, the strengthening of relations with allies, an effective presence in the Indo-Pacific, global peace and stability, the security of missions abroad, the strengthening of the sanctions regime, and countering threats such as terrorism, violent extremism, authoritarianism, transnational organized crime and geopolitical threats (Global Affairs Canada, 2025). Accordingly, a terrorist group constitutes a "policy priority" for Canada where it can threaten one of these interests directly or through intermediary networks.

In order to raise threat assessment from the level of describing groups to the level of policy decision-making, this policy paper proposes the "Canadian Threat-to-National Interest Transmission Matrix". The logic of this matrix is that a terrorist group or violent network becomes a policy priority for Canada when it can be shown through which specific pathway it harms which Canadian national interest.

This matrix helps the Government of Canada to distinguish between direct, indirect, inspirational, facilitating and disruptive threats. Its advantage is that it converts counter-terrorism policy from a purely listing-centred approach into an interests-centred and action-centred one. Within this framework, terrorist listing remains important but is not sufficient, because some networks operate through propaganda, cryptocurrency, hawala, pressure on the diaspora, cyber attack, disruption of shipping or proxy links, without always being identifiable in the classical form of a hierarchical organization.

Table 1: Canadian Threat-to-National Interest Transmission Matrix

Threat actor	Operational capability	Transmission pathway to Canada	National interest at risk	Canadian response tool	Responsible institution	Early-warning indicator
Islamic State Khorasan Province / ISKP	High	Online recruitment, inspiration, Central Asian networks, external attack, multilingual propaganda	Security of citizens, security of missions abroad, social cohesion, credibility with allies	Multilingual monitoring, Five Eyes cooperation, early intervention to assist vulnerable youth,	CSIS, RCMP, CSE, Public Safety, GAC	Increase in Persian/Dari, Pashto, Tajik, Uzbek, Urdu and Russian propaganda; direct or symbolic reference to Canada or its allies

Threat actor	Operational capability	Transmission pathway to Canada	National interest at risk	Canadian response tool	Responsible institution	Early-warning indicator
				cooperation with platforms		
Al Qaida and AQIS	Medium to high	Training, advice, links with Afghanistan–Pakistan networks, ideological inspiration, connection with local groups	Canada's external security, diplomatic missions, security of allies, prevention of the reconstitution of a terrorist safe haven	Afghanistan–Pakistan monitoring, intelligence cooperation with allies, analysis of facilitator networks	CSIS, GAC, DND, Public Safety	Increase in operational messaging, movement of leaders, links with the TTP or local networks, signs of a focus on external operations
Tehrik-e-Taliban Pakistan / TTP	Medium to high	Instability in Pakistan, safe havens in Afghanistan, Kabul–Islamabad tension, effect on migration and the diaspora	Regional stability, security of allies, migration policy, Canada's diplomatic interests	Afghanistan–Pakistan desk at GAC, dialogue with the United Kingdom and the European Union, monitoring of the Afghanistan–Pakistan border, coordination with IRCC in crisis scenarios	GAC, CSIS, DND, IRCC	Increase in cross-border attacks, Kabul–Islamabad diplomatic crisis, threats against foreign or sectarian targets in Pakistan
Haqqani Network and Taliban facilitation	Medium	Provision of safe haven, political protection, facilitation of contact among terrorist groups, ambiguity between governance and jihadist network	Preventing Afghanistan's return to being a terrorist safe haven, humanitarian assistance, safe exit of vulnerable individuals, women's rights	Limited, technical and conditional contact; humanitarian authorization regime; targeted sanctions; multilateral pressure	GAC, Public Safety, CSIS, IRCC	Increased freedom of movement for groups, appointment of hardline figures, restrictions on humanitarian access, increased contact with Al Qaida or the TTP
ETIM/TIP, IMU and Central Asian networks linked to ISKP	Medium	Language, migration, the Russia/Türkiye /Afghanistan route, sleeper cells, Tajik/Uzbek/Russian propaganda	Canada's domestic security, security of European allies, social cohesion, regional knowledge	Establishment of Canada Khorasan–Levant Early Warning Hub, cooperation with Europe and Central Asia, multilingual monitoring	CSIS, GAC, CSE, Establishment of South and Central Asia–Middle East joint analytical cell for Canada	Increase in Tajik, Uzbek and Russian propaganda; return of fighters; concern on the part of Tajikistan, Uzbekistan or European states
Regional proxy groups	High	Threat to the diaspora, transnational repression, financing, cyber	Domestic security, human rights, cyber security, shipping and maritime	Sanctions, listing, diaspora protection, countering foreign	GAC, Public Safety, FINTRAC, CSE, RCMP, CSIS	Threats against activists, extortion, suspicious transactions, cyber attacks, influence or

Threat actor	Operational capability	Transmission pathway to Canada	National interest at risk	Canadian response tool	Responsible institution	Early-warning indicator
		dimensions, political influence, maritime threat	trade, credibility of Canada's foreign policy	interference, financial and cyber tracking		intimidation operations against all communities
Hizballah and affiliated financial/political networks	Medium to high	Financing, front charity or commercial networks, regional links, diaspora pressure	Financial security, social cohesion, Canada's relations with allies, enforcement of the sanctions regime	FINTRAC typology, cooperation with banks, law enforcement, cooperation with Europe and the Middle East	FINTRAC, RCMP, CSIS, Public Safety, GAC	Suspicious financial transfer patterns, front charities, opaque commercial networks, increased Lebanon/Israel tension
Hamas and Palestinian Islamic Jihad	Medium	Social polarization, financing, online propaganda, the reverberation of the Middle East war inside Canada	Social cohesion, security of Jewish and Muslim communities, foreign policy, public order	Law enforcement, protection of vulnerable communities, financial monitoring, balanced and rights-based diplomacy	Public Safety, RCMP, FINTRAC, GAC	Increase in hate propagation, suspicious fundraising, threats against religious sites or civic gatherings
Ansarallah / the Houthis	Medium	The Red Sea, energy security, insurance, supply chain, attacks on shipping	Economy, trade, maritime security, energy prices, Canada's credibility with allies	Maritime cooperation with the United Kingdom, France, the European Union, Japan and Australia; sanctions and listing	DND, GAC, Public Safety	Attacks on vessels, rising insurance costs, disruption of trade routes, threats against allies' vessels
Remnants of the Islamic State in Iraq and Syria	Medium	Inspiration, prisoners and camps, the return or transfer of associated individuals, online propaganda	Domestic security, criminal justice, protection of children, Canada's legal credibility	A clear repatriation policy, security assessment, prosecution, rehabilitation and monitoring	GAC, Justice Canada, RCMP, CSIS, Public Safety	Prison escapes, collapse of camp security, increase in Islamic State propaganda, crisis in northern Syria

This matrix[2] shows that the terrorist threat to Canada is not a linear phenomenon; rather, it is transmitted to national interests by various routes. For example, Islamic State Khorasan Province

[2] The assessments given in the "Operational capability" and "Early-warning indicator" columns are the author's analytical judgment on the basis of the sources cited in this document, not measured data. The three-point scale "High / Medium to high / Medium" expresses a relative assessment of the combination of capability and stated intent, and has no numerical threshold.

may connect to Canada's domestic security through the pathway of multilingual propaganda and online inspiration; the TTP may affect Canada's diplomatic and migration interests through the pathway of instability in Pakistan and Afghanistan–Pakistan tension; and Ansarallah may link to the political economy of Canada's national security through the pathway of the Red Sea, insurance, energy and the supply chain. These three examples are not equal in the strength of their evidence: the second and third pathways rest on observable events, whereas the first relies on a probabilistic assessment. For that reason, Canada's response must also be multi-level: intelligence, financial, cyber, diplomatic, defence, social and legal.

The practical application of this matrix is that it be updated every 90 days by an interdepartmental mechanism and serve as the basis for decision-making on listing, sanctions, diaspora protection, cooperation with allies, the allocation of intelligence resources, and the design of prevention programs. The 90-day period is proposed so that it aligns with the periodic reporting cycle of partner institutions; this period should be reviewed after the first year based on implementation experience. Such an instrument allows Canada neither to fall into threat inflation nor to recognize emerging threats too late. The principal criterion will be each actor's direct and demonstrable relation to Canada's national interests, and not merely notoriety, ideology or external political pressure.

The appropriate criterion for prioritizing threats therefore rests on four pillars: intent to conduct external operations, actual capability, the existence of a link or access pathway to Canada, and the capacity to generate domino effects on the economy, the diaspora or alliances. These four criteria do not replace listing; they complement it and perform a different function: listing determines legal status and executive authorities, whereas these four criteria determine the priority for allocating analytical and policy resources. Separating these two functions resolves the apparent contradiction between "the insufficiency of the listing logic" and "reliance on listing status". For example, the BLA matters for regional security and for the economic interests of Canada's partners, but because it is not listed in Canada, Canada's response should rely more on intelligence, protective cooperation and targeted examination of financing than on mechanical imitation of listing models. By contrast, the TTP, ISKP, AQIS, the Haqqani Network, the IRGC and its Qods Force, Ansarallah, Al Qaida and Lashkar-e-Tayyiba have a clearer legal status, because they are listed on Canada's official list of terrorist entities (Public Safety Canada, 2025a).

Another central assumption of this policy paper is that "absolute reliance on the American umbrella" is no longer a sufficient basis for designing Canada's security policy. Although Canada's official documents still emphasize the renewal of the economic and security relationship with the United States, at the same time, in their security documents, they state explicitly the necessity of strengthening relations with the United Kingdom, Australia, New Zealand, the European Union and other G7 partners. In 2026 as well, credible reports indicate Washington's pressure on Canada to increase its defence share, a pause in part of the bilateral defence dialogues, and a demand for greater European and Canadian participation in NATO capabilities. This does

not mean that the United States has "exited"; it means that Canada must prepare for greater asymmetry within the alliance and build the capacity that is called "hedging" in the international relations literature. It must be stated explicitly that this argument is not inconsistent with the document's simultaneous reliance on the Five Eyes: within this framework the Five Eyes remains the principal foundation, and the "second layer" is not a substitute for it but an addition to it that reduces the cost of a possible disruption in a single channel (Public Safety Canada, 2025c; Reuters, 2026b; Associated Press, 2026b).

Threat Map: Afghanistan, Pakistan, Central Asia and the Middle East

Since 2021, Afghanistan has not only witnessed the rule of a religious extremist group but has also, according to the report of the United Nations Security Council (February 2026), become a regional facilitating environment for several extremist and fundamentalist networks, particularly the TTP. According to the same report, Al Qaida also benefits from Taliban support and acts as a provider of training and advice to other groups, especially the TTP; AQIS has remained active in southeastern Afghanistan and has acquired a greater focus on external operations; Islamic State Khorasan Province, despite counter-terrorism pressure, still has "strong capability" and "the intent to conduct external operations" and has expanded its cellular network for regional and extra-regional threat; and ETIM/TIP, with Taliban support, has become more concentrated in Badakhshan and has gained greater freedom of movement (United Nations Security Council, 2026). From the standpoint of Canadian law, however, a distinction must be drawn between these groups: the Haqqani Network, the Taliban, Al Qaida, AQIS and ISKP are listed on Canada's list of terrorist entities; but ETIM/TIP is not included on this list, and this document's reference to it rests on the assessment of the UN Monitoring Team, not on its legal status in Canada (Public Safety Canada, 2025a).

Pakistan's role in this regional threat environment likewise has two simultaneous aspects that must be distinguished from one another. On the one hand, Pakistan's security policies towards the Taliban and other regional paramilitary networks have long been contested and the subject of allegations in the security literature and in Pakistan's relations with its neighbours; on the other hand, and paradoxically, Pakistan has now, by the measure of open global indices, become the country most affected by terrorism. The "Global Terrorism Index 2026" reports that for the first time Pakistan ranked first among the countries most affected by terrorism, with 1,139 killed and 1,045 terrorist incidents in 2025; this jump is specifically linked to the Taliban's return to power, the increase in TTP violence and the activity of the BLA. In the same report, the TTP is identified as one of the four principal deadliest groups in the world in 2025 and is the only one among those four to have recorded an increase in its lethality (Institute for Economics & Peace, 2026). The UN report likewise records an increase in TTP attacks against Pakistan and the fragility of regional relations. At the level of events, the deadly TTP attacks in the Afghanistan–Pakistan border areas in February 2026 and the Islamic State attack on a Shia mosque in Islamabad showed that Pakistan

is simultaneously engaged with two types of threat: an anti-state jihadist insurgency, and the sectarian/brand-building attacks of the Islamic State (United Nations Security Council, 2026; Reuters, 2026a; Associated Press, 2026a; Institute for Economics & Peace, 2026).

Although Central Asia occupies a smaller place in this threat architecture, it is not marginal. The UN report states explicitly that the aggressive propaganda of Islamic State Khorasan Province has recently expanded into Central Asian languages, that this group has members from almost all of the region's ethnic groups, and that countries such as Tajikistan and Uzbekistan are concerned about the growing role of their nationals within the Islamic State Khorasan Province structure and about the formation of "sleeper cells".[3] In addition, ETIM/TIP[4] has created a trans-spatial link in Afghanistan and Syria that affects the mobility of foreign fighters and the future of the region's security (United Nations Security Council, 2026). In policy terms, Central Asia is for Canada not merely a "distant space" but also a potential source of linguistic, cyber, migration and extraterritorial threats and of inspiration for external operations.

In the Middle East, a distinction must be drawn between "attack-executing groups" and "supporting groups/facilitating axes". From Canada's standpoint, the IRGC is now formally listed as a terrorist entity, and the Government of Canada has described it as the principal actor connecting the Iranian regime to regional proxy groups, including Hizballah and Hamas. Ansarallah has likewise been on Canada's list since December 2024, and the Government of Canada's official description of it emphasizes both its alignment with the "axis of resistance" and its disruptive attacks on commercial and naval vessels in the Red Sea. In addition, it should be noted that the IRGC and the Qods Force are official organs of a state; the instruments for responding to them are not the same as the instruments for responding to a non-state network. This raises questions relating to state immunity and diplomatic law. The UN report also shows that AQAP has become more dynamic within Al Qaida's global network and that its external threat is assessed to be increasing; in Syria, jihadist structures likewise remain fluid, Hurras al-Din announced its dissolution in January 2025, but questions are still raised about the loyalty of its former members to Al Qaida's global agenda, and ETIM/TIP has been integrated or semi-integrated into the new military structures (Public Safety Canada, 2025a; United Nations Security Council, 2026).

A Balanced Assessment: What the Data Does Not Support

Methodological fairness requires that two findings in the same "Global Terrorism Index 2026" on which this document relies, both of which run counter to its general narrative, be stated explicitly.

---

[3] This concern is those states' stated assessment and is not treated in this document as an established fact.

[4] The author is committed to the position that caution must be exercised in using the label ETIM/TIP: the organizational status of this label is the subject of international dispute, and some states have removed it from their lists on the grounds of insufficient evidence of continued organizational existence. This document cites this label solely as a category used in United Nations reports and draws no conclusion from it about Uyghur communities in Canada.

First, that for the first time since the inception of this index, Afghanistan has dropped out of the list of the ten countries most affected by terrorism. Second, that Canada's score on the same index is 1.333, that is, at a level close to the floor of the scale and among the countries with the least direct impact (Institute for Economics & Peace, 2026).

These two findings should not be belittled; but they do not refute this document's argument, rather they make its scope more precise. The Global Terrorism Index measures incidents and casualties. What it does not measure is three things that are precisely the subject of this document: the capacity of an environment to facilitate third-party groups; intent to conduct external operations that have not yet been acted upon; and the transmission of risk through financial, digital and diaspora pathways that are not recorded in attack statistics. The decline in the number of attacks in Afghanistan is not inconsistent with the UN Monitoring Team's report of the persistence of a facilitating environment and of the retention by Islamic State Khorasan Province of "strong capability and the intent to conduct external operations" (United Nations Security Council, 2026); the two measure two different things.

Canada's low score is likewise precisely the point from which this document begins: the direct and actual threat against Canadian territory is low, and the national threat level has remained unchanged for more than a decade. The document's argument does not rest on an increase in the intensity of the threat, but on the proposition that the mix of transmission pathways has changed and that the existing assessment apparatus, designed mainly to measure the threat of direct attack, does not see this change in full. In other words, the score of 1.333 is a measurement of past success, not a guarantee of the future; the policy question is therefore this: is the current architecture sufficient to maintain that same score in an environment with more diverse pathways of insecurity?

For this reason, this policy paper does not speak of raising the national alert level and makes no recommendation premised on crisis urgency. Its recommendations are mainly of the order of process reform, institutional coordination and analytical capacity-building, that is, of the order of measures that, under conditions of a medium and stable threat, constitute the most rational investment for managing future crises and threats.

Linking Threats to Canada's National Interests

The first link is with territorial security and the security of Canadian citizens. Canada's national threat level remains MEDIUM, and the government's official assessment states that ITAC monitors terrorist threats against "Canada and Canadian interests globally". When the United Nations speaks of "strong capability together with the intent to conduct external operations" in relation to Islamic State Khorasan Province, or reports increasing concern about external operations in relation to AQIS (Government of Canada, 2025; United Nations Security Council, 2026), that warning is relevant to Canada as well; because the logic of these groups operates beyond local borders, and Canada too has citizens, diplomatic missions, flights, international trade,

institutions and economic relationships abroad. It must be stated explicitly that this argument establishes that Canada is not exempt, not that it is specifically targeted; establishing targeting requires the presentation of separate Canadian evidence, to which later sections of this policy paper will refer.

The second link is the protection of the diaspora and social cohesion within Canada. A common strategic error is to view migration from the regions studied in this policy paper solely through the lens of risk, whereas the real issue is the simultaneous protection of open Canadian society and of immigrant communities against intimidation, coerced financing, extremist mobilization, threats against activists and extraterritorial assassination. Public Safety Canada's 2025 transition documents explicitly place countering foreign interference, the protection of democratic institutions, countering misinformation, online harms and ideologically motivated violent extremism at the centre of cooperation with the United Kingdom, the Five Eyes and the G7. The final report of the Foreign Interference Commission had likewise warned that public unawareness, misinformation and intimidation originating from foreign actors weaken trust in and the health of Canadian democracy (Morris, 2025; Public Safety Canada, 2025c; Reuters, 2025a).

The third link is economic security, supply chains and critical infrastructure. If Canadian counter-terrorism policy remains focused solely on preventing physical attack on Canadian soil, it will be insufficient. Ansarallah's attacks on shipping and the crises of the Middle East have shown that an actor or quasi-proxy group can raise energy prices, transport insurance and the cost of trade through disruption of maritime passages. The magnitude of this effect on Canada, which is itself a net energy exporter and has a limited direct share in Red Sea trade, requires separate quantitative measurement and is presented in this document as a potential pathway, not a measured effect. Domestically, Global Affairs Canada in its 2025–2026 plan has emphasized supply chain resilience, the security of missions, and the protection of critical infrastructure and classified networks. Terrorism is therefore not only a question of "police and borders" for Canada; it is also a question of "the political economy of national security" (Global Affairs Canada, 2025; Public Safety Canada, 2025c).

The fourth link is the credibility of alliances and the necessity of security diversification. The official Public Safety document states that Canada's most important security counterparts, after the United States, are the United Kingdom and then Australia and New Zealand, and that the G7 and Five Eyes frameworks are the pillars of cooperation. At the same time, 2026 reports indicate increasing US pressure for Europe and Canada to fill capability gaps in NATO. Canada's fight against terrorism should therefore be designed from the outset in connection with defence diplomacy with the United Kingdom, France, Germany, the Netherlands, the Nordic countries, Australia, New Zealand and Japan; not as a complete substitute for the United States, but as a second layer of capability and a first layer of strategic resilience (Public Safety Canada, 2025c; Reuters, 2026c; Associated Press, 2026b).

The fifth link is cyber and information security. This pathway is reflected in three other places in this same document: in Table 1, "cyber" is listed as one of the transmission pathways of the proxy groups in the Middle East; in Pillar Five, the tracking of virtual assets and of multilingual propaganda on platforms is identified as a regulatory priority; and in Pillar Seven, combined terrorism/cyber exercises are treated as part of the doctrine of continental resilience. The policy synthesis of these three is that cyberspace has three functions simultaneously: a channel for recruitment and propaganda, an instrument for transferring financial value, and an attack surface against infrastructure. Canada's response on this link cannot therefore be merely the technical defence of networks; it must bring financial regulation, open-source monitoring and infrastructure protection together within a single framework. It should be added that distinguishing between an attributable cyber attack and non-attributable propaganda penetration is a necessary condition for the correct allocation of resources in this area.

Canadian Evidence of the Threat

Up to this point, the argument of this policy paper has rested on regional evidence. But a model whose name is "transmission of threat to Canada's national interest" moves beyond the level of a conceptual framework only when it shows that this transmission is observable in Canada itself. The available data present a picture that is specific and at the same time limited; on the dimension of the recruitment and radicalization of young people, the 2025 public report of CSIS states that close to one in ten of the organization's terrorism investigations involves at least one person under eighteen years of age; in Canada, five minors were arrested in 2023, two in 2024 and four in 2025. The same report states explicitly that at least seven of the organization's priority investigations concerning mobilization to violence have been assessed as being wholly or partly influenced by the Middle East war, and that two returned Canadian extremist travellers were convicted in 2025 on charges of participating in the activities of a terrorist group (the Islamic State) (CSIS, 2026).

But this same source introduces an important qualification to this document's narrative, which must be stated explicitly: the assessment of CSIS indicates that the concentration of youth radicalization in Canada lies mainly in online neo-Nazi and nihilistic violent extremism ecosystems, and not solely in narratives arising from the geography discussed in this document. The implication of this finding for the "transmission pathway" model is twofold. On the one hand, it rejects the simplistic assumption that would attribute the online recruitment of young people in immigrant communities mainly to the propaganda of Islamic State Khorasan Province or Al Qaida. On the other hand, it confirms the logic of the model itself: if the unit of analysis is the "pathway" and not the "group's geography", then the pathway of online recruitment of adolescents, irrespective of its ideological origin, is a single pathway with similar mechanisms. For this reason, this document recommends that early intervention programs be designed based on the recruitment mechanism and not on the basis of the ideology of origin.

On the dimension of direct attack, the case of the July 2024 arrests in the Greater Toronto Area is a notable example: two accused were prosecuted on charges of conspiracy to commit murder on behalf of the Islamic State, and one of them also faces a separate Islamic State-related charge concerning an incident outside Canada in 2015. This case shows that the "inspiration and organizational connection" pathway is not merely hypothetical (Public Safety Canada, 2024).

What the Canadian data confirm is the existence of three active pathways: the online recruitment of young people (with an ideological composition different from what this document's geographic focus would suggest), connection to the Islamic State at the level of criminal cases, and state transnational repression. What these data do not confirm is the magnitude of these pathways or their primacy over other threats. Other pathways that this document raises, including the effect of shipping disruption on Canada's economy and the link between Central Asian networks and Canada's domestic security, at present have no direct Canadian evidence, owing to the absence of independent and coherent research, and are therefore presented in this document as a potential pathway.

Existing Gaps in Canadian Policy

The first gap is the dominance of the listing logic over the logic of network analysis. In 2024 and 2025 Canada took several major steps: it listed the IRGC, added Ansarallah, and in December 2025 listed four new entities, including 764, the Terrorgram Collective and Islamic State-Mozambique. These measures were important, but they appear insufficient to contain potential threats; because many threat networks operate through media, logistics, financial intermediaries, commercial covers, intermediate actors or inter-regional links that are not necessarily visible in classical lists. Another notable point is that two of the four entities added in December 2025 belong to online accelerationist networks and not to the geography discussed in this document; this shows that the "transmission pathway" logic that this document proposes has a scope extending beyond regional threats. Even in the case of emerging youth-centred threats, the Government of Canada itself has acknowledged that the online dimension and the radicalization of young people must be seen as a principal front, not a marginal one (Public Safety Canada, 2025b).

To this picture must be added another structural fact that is itself the strongest evidence for this policy paper's argument: Canada's national counter-terrorism strategy, under the title "Building Resilience Against Terrorism", dates from 2012 and is still the guiding document for more than twenty federal departments and agencies (Public Safety Canada, 2012). This strategy was written before the rise and fall of the Islamic State caliphate, before the Taliban's return to power in 2021, before the emergence of Islamic State Khorasan Province as an external-operations actor, before the online radicalization of adolescents in its present form, before crypto-asset-based financing, and before transnational repression became an independent policy agenda. The National Strategy on Countering Radicalization to Violence, which complements it, likewise dates from 2018 (Public Safety Canada, 2018). The distance between the date of these documents and the 2026 threat

environment by itself explains why the listing logic dominates the logic of network analysis: Canada's policy-making apparatus still works on the basis of a framework that was designed for the threat environment of a decade and a half ago.

The second gap is the distance between counter-terrorism policy and assistance/field-presence policy. The experience of Afghanistan after 2021 and the return of the Taliban showed that if the legal framework is not flexible, Canada either withdraws from high-risk environments and becomes "blind", or faces the risks of unintended financing. The official 2025 annual report on the authorization regime for activities in geographic areas controlled by a terrorist group was created precisely to resolve this contradiction: humanitarian assistance and other essential activities must remain possible, while security assessment and financial control are also maintained (Public Safety Canada, 2025d). Nevertheless, this regime is still seen mainly as an instrument of legal/humanitarian compliance, not as a strategic instrument for preserving legitimate presence, field understanding and network-building with local partners in terrorism-affected environments.

The third gap is the absence of a comprehensive approach to protecting the diaspora against the overlap of terrorism, foreign interference and transnational repression. In practice, these three areas are often not separate in actual cases: a state or proxy group can intimidate, demand financing, collect intelligence and build a radical propaganda space all at once. Nevertheless, the empirical overlap of these three phenomena does not mean that they are legally identical: in Canadian law each activates different authorities, evidentiary thresholds and oversight regimes. What this document means by "integration" is operational coordination and a single reporting channel for the victim, not the merger of the legal bases of these three areas. But Canada's institutional architecture still tends to distribute these matters among the RCMP, CSIS, GAC, IRCC and local institutions (Public Safety Canada, 2025c; Reuters, 2025a; Morris, 2025). This fragmentation both makes reporting by victims difficult and fails to produce a single picture of risk. To this must be added that in June 2024 Canada took an important institutional step by passing the "Countering Foreign Interference Act" and, among other things, created the Foreign Influence Transparency Registry (Parliament of Canada, 2024). This Act covers part of the gap, but its focus is on interference in democratic processes and not on the operational protection of individuals who are the target of transnational repression; the distance between these two is precisely where this policy paper's proposal is situated.

The fourth gap has been excessive dependence on American intelligence and operational leadership. As long as NORAD and the Five Eyes remain in place, this dependence has not been entirely severed; but the pressures of 2025–2026 show that if Canada does not pursue greater analytical independence, language coverage, cyber capacity and operational partnership with non-US allies, it will remain vulnerable when facing simultaneous crises in the Middle East, Afghanistan–Pakistan and the online space (Public Safety Canada, 2025c; Reuters, 2026b).

Proposed Framework and Practical Recommendations

The principal proposal of this policy paper is the establishment of a framework of "network-centred counter-terrorism for Canada's national interests", resting on seven pillars. The relation of these seven pillars to the four identified gaps is as follows:

Pillar One and Pillar Five respond to the first gap (the dominance of the listing logic); Pillar Two to the second gap (the distance between counter-terrorism and field presence); Pillar Three to the third gap (the fragmentation of diaspora protection); and Pillar Four and Pillar Seven to the fourth gap (dependence on American leadership). Pillar Six has a cross-cutting function and makes the prioritization logic uniform across all four areas.

Pillar One: Establishment of a South and Central Asia–Middle East joint analytical cell for Canada. This cell should be formed under PCO/NSIA and with the participation of GAC, CSIS, RCMP, FINTRAC, CBSA and CSE, and its mandate should be not only the collection but the "integration" of threat data: the Taliban–Haqqani–Al Qaida–TTP–ISKP relationships; the ETIM/TIP links between Afghanistan and Syria; the region's proxy groups; and the effect of these networks on diasporas within Canada. The advantage of this proposal is that it converts a case-centred logic into a network-centred one and links threat assessment directly to national interests. This proposal requires no new legal authority and is implementable through an interdepartmental coordination decision under PCO/NSIA; but before implementation its relation to ITAC's mandate must be clarified so that it does not lead to duplication (United Nations Security Council, 2026; Public Safety Canada, 2025a).

Within this pillar, another important proposal of this policy paper is the establishment of a "Canada Khorasan–Levant Early Warning Hub": a small, pilot, multilingual and interdisciplinary body capable of reducing the gap between academic research, policy analysis and security assessment in the field of threats arising from Afghanistan, Pakistan, Central Asia and the Middle East. In its first phase, this hub could be designed with the hosting or participation of the University of Ottawa or Carleton University,[5] and in structural coordination with Global Affairs Canada, Public Safety Canada, CSIS, CSE, FINTRAC, DND and RCMP; the rationale for establishing this hub is that today's threats no longer remain within a closed geography. Islamic State Khorasan Province, Al Qaida, Al Qaida in the Indian Subcontinent, Tehrik-e-Taliban Pakistan, ETIM/TIP, the Central Asian networks, the remnants of the Islamic State and Al Qaida in Syria and Iraq, and the proxy groups in the Middle East are connected to one another through linguistic, digital, financial, diaspora, migration, cyber and geopolitical pathways. Khorasan and the Levant are not, within this framework, two separate geographies; they are two poles of a single threat ecosystem extending from Afghanistan and Pakistan to Central Asia, Syria, Iraq, Yemen, Iran and Türkiye. For Canada, the importance of this ecosystem is that threats can emerge not only in the form of direct attack

[5] Since the author of this document is affiliated with the Universities of Ottawa and Carleton, and this proposal raises the hosting of one of these two universities, that affiliation is declared explicitly; assessment of the merit of the proposal should be conducted independently of this institutional relationship.

but also through online extremism, micro-financing, cryptocurrency, pressure on the diaspora, transnational repression, supply chain disruption and threats against allies. The value added by this hub is that it moves Canada from a posture of post-crisis reaction to one of early warning.[6]

Pillar Two: Converting the authorization regime for activities in geographic areas controlled by a terrorist group into a strategic instrument. For example, a country such as Afghanistan should not become for Canada a "moral and informational blind spot". The 2025 authorization regime shows that Canada can strike a balance between the prohibition on terrorist financing and the continuation of essential activities. That is, through a legal, transparent and humanitarian presence in environments such as Afghanistan and Syria, it emerges from policy blindness and, at the macro level, gains a better understanding of human, financial, migration and security risks. Of the seven pillars, this pillar has the lowest cost and the least need for new legal authority, because its subject is process reform within an established regime and not the creation of a new institution.

The practical recommendation is that GAC and Public Safety create, for the Afghanistan, Syria and other comparable files, a faster, more transparent and mandate-driven pathway for accredited Canadian organizations (Public Safety Canada, 2025d) such that each authorization encompasses not only compliance considerations but also the value added in human security, information access, field knowledge and the reduction of competitors' influence.

Pillar Three: A dedicated strategy for protecting the diaspora without identity securitization. Canada should establish a "National Protocol for the Protection of Communities Exposed to Transnational Repression and Cross-border Extremism". Its components should include a secure reporting channel, coordination between federal and local police, witness support, legal advice, training for community institutions, and multilingual liaison teams. The criterion of inclusion in this protocol should be "being exposed to a threat" and not ethnic or national belonging; that is, a person is covered by protection because they are targeted, not because of their country of origin. This specification is both more consistent with section 15 of the Canadian Charter of Rights and Freedoms and more precise, because transnational repression targets specific individuals and not communities as a broad whole. This policy should emphasize explicitly that immigrant communities are the object of protection, not the object of collective suspicion. This aligns precisely with Canada's priorities in countering foreign interference, misinformation, online harms and extremism (Public Safety Canada, 2025c).

Terrorism, foreign interference and transnational repression are often not separate in actual cases, and they are dispersed among different Canadian institutions. On this basis, the "Diaspora Protection and Partnership Compact" is considered one of the central proposals of this policy paper.

---

[6] A separate document will be written on the necessity, mandate, structure and mechanism of this hub and on how it links to Canada's national interests and national security.

This compact should cover three types of threat simultaneously. First, extremism and online recruitment, especially among vulnerable young people who may be targeted through the narratives of Islamic State Khorasan Province, Al Qaida, sectarian extremist groups, ideologically motivated violent networks or digital propaganda. Second, coerced financing, extortion, network pressure and threats against families; that is, a situation in which individuals in Canada are compelled, through threats against their families in the country of origin, social pressure, ethnic/religious networks, hawala, front charities or commercial relationships, to pay money, to remain politically silent or to cooperate unwillingly. Third, transnational repression by states or proxy groups; a threat that can include assassination, harassment, physical threats, digital stalking, doxing, legal abuse, threats against relatives in the country of origin, social exclusion, influence operations, extortion, and the intimidation of activists, journalists, students, human rights defenders and political opponents. The 2025 CSIS public report likewise defines transnational repression as an attempt by foreign states or their agents to threaten, harass, harm or silence individuals and communities beyond their borders, and refers to tactics such as threats against relatives, legal abuse, social ostracism, malicious digital activity and extortion (CSIS, 2026). This is also consistent with the G7 position, which regards transnational repression as a threat to national security, the sovereignty of states, human rights and the principles of international law (G7, 2025).

The value added by this compact is that it moves Canada's counter-terrorism policy from the stage of "reaction after the incident" to the stage of "protection and early prevention". A family worried about the radicalization of its child, a human rights activist threatened by a foreign network, a migrant under pressure to pay money to an armed or proxy group, or a journalist whose family in the country of origin is threatened, should not be left between silence, fear and direct recourse to security institutions without community support. Canada needs a middle path: one that takes law and security seriously while also preserving the trust, dignity, privacy and participation of immigrant communities.

Pillar Four: Diversified security diplomacy with non-US allies. The United Kingdom should be Canada's first partner in this package, because the official Public Safety document calls it Canada's closest security ally after the United States. After that, Australia and New Zealand within the Five Eyes, and Japan, France, Germany, the Netherlands and the Nordic countries within the G7/NATO/thematic coalitions, should be prioritized.

This policy paper proposes that Canada design a multi-domain counter-terrorism minilateral organized around the themes of "youth-centred online threats", "the languages of Central and South Asia", "diaspora protection" and "shipping and supply chain security". This initiative could both compensate for the void created by a relative reduction in reliance on the United States and increase Canada's norm-setting role. Two implementation considerations must be taken into account from the outset within this framework: first, that the value added by this initiative relative to existing multilateral channels must be demonstrated explicitly, otherwise potential partners will have no reason to join; second, that the composition of partners in each cluster carries political

consequences, and their selection must be deliberate and made with an assessment of bilateral sensitivities (Public Safety Canada, 2025c; Reuters, 2026b).

In this connection, emphasis is placed on the diversification of intelligence partners.

Pillar Five: A focus on the infrastructure that supports terrorism, not only on armed cores. The Government of Canada should use its listing, sanctions, financial monitoring and law enforcement capacities to target "media, crypto-assets, logistical intermediaries, commercial covers, and recruitment and propaganda circles". The UN report warns that terrorist groups are using commercial satellite communications and artificial intelligence for better propaganda, recruitment and coordination. In addition, in 2025 FATF warned that regulatory gaps in virtual assets globalize the risk of terrorist financing. Canada should therefore focus, both domestically and at the G7/Five Eyes level, on tracking stablecoins, virtual asset services and multilingual propaganda on platforms. In implementing this pillar, a foreseeable side effect must be managed: intensified monitoring of hawala channels could make the cost of and access to money transfers difficult for the very immigrant communities that Pillar Three seeks to protect. Measuring this effect must be part of policy design (United Nations Security Council, 2026; Reuters, 2025b).

Within the framework of this financial monitoring, it is desirable that greater attention be paid to the following:

- small but repeated transactions to high-risk regions;
- the combined use of hawala, charities, exchange houses, cryptocurrency and cash;
- unhosted wallets;
- stablecoins on low-cost networks;
- micro-financing by young people or self-starting cells;
- the exploitation of humanitarian crises for fundraising.

Pillar Six: Legal-policy differentiation among groups, but operational integration of the response. The basis of this classification is the same four criteria set out earlier: intent to conduct external operations, actual capability, the existence of an access pathway to Canada, and the capacity to generate domino effects. On this basis, the TTP, ISKP, AQIS, the Haqqani Network and the proxy groups fall within the "first threat class", because they possess both capability and cross-border links. Ansarallah and AQAP fall within the "second, disruptive threat class", because they affect shipping, energy and extra-regional inspiration. The Taliban–Haqqani facilitating environment, in accordance with the distinction set out in earlier sections of this document, falls within the separate category of "facilitator" and not within the operational threat classes; the instrument appropriate to it is limited, technical and conditional contact, not operational action. The BLA and similar actors fall within the "conditional threat class": monitoring, financial analysis and protective cooperation regarding them should be intensified, but any legal step must necessarily rest on

Canada's official criteria and precise evidence, not on geopolitical haste. This classification helps Canada neither to see threats as flat nor to administer the response apparatus in a fragmented way (Institute for Economics & Peace, 2026; Public Safety Canada, 2025a; United Nations Security Council, 2026)

Pillar Seven: Linking counter-terrorism to Canada's continental defence doctrine and national resilience. If the United States is placing a greater burden on its allies, Canada must move counter-terrorism from the margin to the centre of its defence program and economic security: the security of ports and airports, the protection of energy and telecommunications infrastructure, combined terrorism/cyber exercises, scenarios of disruption to global shipping, and the protection of missions abroad. This aligns precisely with the government's official priorities in strengthening NORAD, the security of missions abroad, the protection of classified networks and a new security relationship with the United States and other allies (Global Affairs Canada, 2025; Reuters, 2026b).

If these seven pillars are translated into operational language, a realistic action map for the next two years could be as follows: in the first six months, establishment of the joint analytical cell, drafting of the threat classification matrix, and reform of the authorization regime process; at twelve months, launch of a pilot of the diaspora protection protocol and design of the minilateral initiative with the United Kingdom–Australia–New Zealand–Japan, together with a joint package on online threats and the region's languages; and at eighteen to twenty-four months, linking the output of these mechanisms to decision-making on listing, targeted sanctions, the protection of critical infrastructure, and the redesign of Canada's diplomatic/development presence in high-risk environments.

In this sequence, Pillar Two has no real prerequisite and can begin immediately; by contrast, the Khorasan–Levant Early Warning Hub and the policing component of the diaspora protocol are both conditional on legal determination and should not enter the implementation phase before that. The advantage of this model is that it neither becomes trapped in idealism nor slides into crude securitarianism.

Conclusion

This document began from a simple observation and arrived at an architectural proposal. The observation was that the terrorist threat to Canada comes through pathways that the existing assessment apparatus, which rests mainly on identifying a group and placing it on a list, does not see in full. The proposal is that the unit of analysis be moved from "which group is active" to "which group, through which pathway, threatens which Canadian national interest".

Three points must be stated explicitly in conclusion. First, this document does not claim that Canada faces an immediate and growing threat. The national threat level has remained unchanged for more than a decade, and international indices assess Canada's direct impact at a low level. The argument rests on a change in the mix of pathways, not on a change in intensity.

Second, the available Canadian evidence confirms three active pathways: the online recruitment of young people, organizational connection at the level of criminal cases, and state transnational repression; and it is silent on the other pathways. This silence does not mean the absence of a pathway, but it does mean the absence of proof; and the document has preserved this distinction throughout the text. The most important negative finding is also stated explicitly: the concentration of youth radicalization in Canada does not coincide with the geography discussed in this document, and this is a reason for the superiority of the pathway-centred logic over the geography-centred logic.

Third, the most important recommendation of this document is not necessarily its most costly. Reform of the authorization regime for activities in geographic areas controlled by a terrorist group, which is feasible within the existing legal framework and at the lowest cost, has the greatest immediate return: without a legitimate presence in environments such as Afghanistan and Syria, Canada loses not only its capacity to provide assistance but also its capacity to understand. By contrast, the costliest and most sensitive recommendation, namely the diaspora protection compact, should be implemented cautiously, with a limited pilot, with an inclusion criterion based on threat and not identity, and with independent evaluation before expansion.

Ultimately, the real test of any counter-terrorism policy in a multicultural society is whether it purchases security at the cost of trust or builds it upon trust. Canada can choose the second course, not out of idealism, but because in an environment where the threat passes through communities, a distrustful society is the most costly vulnerability possible.

References

Associated Press. (2026a, February 6). Suicide bombing at a Shiite mosque on Islamabad's outskirts kills at least 31 and wounds scores. AP News. Retrieved June 09, 2026, from https://apnews.com/article/pakistan-islamabad-shiite-mosque-blast-8f0b7b8a8783db37644d88610512c9af

Associated Press. (2026b, June 19). Pentagon chief's review appears out of step with what NATO allies are already doing. AP News. Retrieved June 20, 2026, from https://apnews.com/article/nato-us-hegseth-pentagon-review-europe-spending-0529a8f0c581ff34a427a70086223c61

CSIS. (2026). CSIS public report 2025: Operations and analysis. Government of Canada. Retrieved April 26, 2026, from https://www.canada.ca/content/dam/csis-scrs/images/2025/public-report/Public%20Report_EN_2025_DIGITAL.pdf

G7. (2025, June 17). G7 leaders' statement on transnational repression. Prime Minister of Canada. Retrieved August 26, 2025, from https://www.pm.gc.ca/en/news/statements/2025/06/17/g7-leaders-statement-transnational-repression

Global Affairs Canada. (2025). Global Affairs Canada's 2025–26 departmental plan. Retrieved August 23, 2026, from https://international.canada.ca/en/global-affairs/corporate/reports/departmental-plan/global-affairs-2025-2026-departmental-plan

Government of Canada. (2025). Canada's national terrorism threat levels. Retrieved August 23, 2026, from https://www.canada.ca/en/services/defence/nationalsecurity/terrorism-threat-level.html

Institute for Economics & Peace. (2026). Global Terrorism Index 2026: Measuring the impact of terrorism. IEP. Retrieved August 28, 2026, from https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf

Kuik, C.-C. (2016). How do weaker states hedge? Unpacking ASEAN states' alignment behavior towards China. Journal of Contemporary China, 25(100), 500–514. Retrieved June 21, 2026, from https://doi.org/10.1080/10670564.2015.1132714

Kuik, C.-C. (2021). Getting hedging right: A small-state perspective. China International Strategy Review, 3(2), 300–315. Retrieved July 20, 2026, from https://doi.org/10.1007/s42533-021-00089-5

MORRIS, J. (2025, January 28). Canada inquiry found no evidence of 'traitors' in parliament, but warns against disinformation. AP News. Retrieved August 05, 2026, from https://apnews.com/article/canada-foreign-interference-report-traitors-parliament-df7001ea0c76f76fe105869ccec4a420

O'Toole, T., Meer, N., DeHanas, D. N., Jones, S. H., & Modood, T. (2016). Governing through Prevent? Regulation and contested practice in state–Muslim engagement. Sociology, 50(1), 160–177. Retrieved April 15, 2026, from https://doi.org/10.1177/0038038514564437

Parliament of Canada. (2024). Bill C-70: An Act respecting countering foreign interference (Royal Assent, 20 June 2024). Retrieved April 15, 2026, from https://www.parl.ca/legisinfo/en/bill/44-1/c-70

Perliger, A., & Pedahzur, A. (2011). Social network analysis in the study of terrorism and political violence. PS: Political Science & Politics, 44(1), 45–50. Retrieved April 15, 2026, from https://doi.org/10.1017/S1049096510001848

Public Safety Canada. (2012). Building resilience against terrorism: Canada's counter-terrorism strategy. Government of Canada. Retrieved April 19, 2026, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rslnc-gnst-trrrsm/index-en.aspx

Public Safety Canada. (2018). National strategy on countering radicalization to violence. Government of Canada. Retrieved April 15, 2026, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtg-cntrng-rdclztn-vlnc/index-en.aspx

Public Safety Canada. (2024). Parliamentary committee notes: Toronto terror plot arrests. Government of Canada. Retrieved April 15, 2026, from https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20241227/11-en.aspx

Public Safety Canada. (2025a). Currently listed entities. Government of Canada. Retrieved August 18, 2026, from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx

Public Safety Canada. (2025b, December 8). Government of Canada lists four new terrorist entities. Government of Canada. Retrieved April 15, 2026, from https://www.canada.ca/en/public-safety-canada/news/2025/12/government-of-canada-lists-four-new-terrorist-entities.html

Public Safety Canada. (2025c). Transition binder: International engagement. Government of Canada. Retrieved April 15, 2026, from https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20250422/10-en.aspx

Public Safety Canada. (2025d). 2025 annual report of the Minister of Public Safety concerning Criminal Code sections 83.031 to 83.0391. Government of Canada. Retrieved April 16, 2026, from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nnl-prt-crmnl-cd-sctns-83-2025/index-en.aspx

Reuters. (2025a, January 28). Canada responded slowly to foreign meddling, elections were not altered, probe finds. Reuters. Retrieved April 15, 2026, from https://www.reuters.com/world/americas/canada-responded-slowly-foreign-meddling-elections-were-not-altered-probe-finds-2025-01-28/

Reuters. (2025b, June 26). Global financial crime watchdog calls for action on crypto risks. Reuters. Retrieved April 15, 2026, from https://www.reuters.com/sustainability/boards-policy-regulation/global-financial-crime-watchdog-calls-action-crypto-risks-2025-06-26/

Reuters. (2026a, February 17). Militants kill 11 Pakistani security personnel, one child near Afghan border, army says. Reuters. Retrieved April 15, 2026, from https://www.reuters.com/world/asia-pacific/eleven-security-personnel-one-child-killed-militant-attack-pakistan-2026-02-17/

Reuters. (2026b, May 21). Canada falling short on defense spending, F-35 review, Pentagon official says. Reuters. Retrieved June 15, 2026, from https://www.reuters.com/business/aerospace-defense/canada-falling-short-defense-spending-f-35-review-pentagon-official-says-2026-05-21/

Reuters. (2026c, June 17). Allies filling gaps in NATO crisis forces left by US, Rutte says. Reuters. Retrieved June 25, 2026, from https://www.reuters.com/world/americas/allies-filling-gaps-nato-crisis-forces-left-by-us-rutte-says-2026-06-17/

Thrall, A. T., & Cramer, J. K. (Eds.). (2009). American foreign policy and the politics of fear: Threat inflation since 9/11. Routledge.

United Nations Security Council. (2026). Thirty-seventh report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2734 (2024) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities (S/2026/44). United Nations. Retrieved August 15, 2026, from https://www.securitycouncilreport.org/un-documents/document/s-2026-44.php

Université d'Ottawa University of Ottawa

CÉPI **CIPS**

Centre d'études
EN POLITIQUES
INTERNATIONALES



Centre for
INTERNATIONAL
POLICY STUDIES