

RESEARCH ARTICLE

Ideologically Motivated Violent Extremist Financing in Canada

Elena Martynova,* and Jessica Davis

Volume XX, Issue 3
September 2026

ISSN: 2334-3745
DOI: 10.19165/DONY9939

Abstract: Over the past 40 years, ideologically motivated violent extremist (IMVE) attacks have occurred more frequently and caused more deaths and injuries in Canada than any other form of terrorism. This article examines how IMVE groups, attacks, and networks in Canada are financed. Through an analysis of seven groups and eleven attacks, and consideration of transnational networks, a baseline understanding of how groups in Canada raise, use, store, move, obscure, and manage funds, as well as the costs of IMVE attacks, is established. The authors further assess whether counter-terrorist financing (CTF) tools can be applied to the threat of IMVE. Although military approaches are unlikely to be useful, both states and non-state actors have other CTF methods at their disposal to combat IMVE financing, including leveraging financial intelligence, sanctions, and financial deplatforming.

Keywords: counter-terrorist financing, ideologically motivated violent extremism, terrorist financing, policy analysis, right-wing extremism

*Corresponding author: Elena Martynova, Metropolitan University Prague, email: elena.martynova@mup.cz

The nature of terrorism is continuously evolving due to a myriad of factors, including ever-changing counter-terrorism efforts, fluctuating political tensions, and a fragmented and unstable extremist ecology.¹ How terrorism is conceptualised also changes, with contemporary terrorism described in terms such as lone actors, leaderless movements, and decentralised networks.² As a result of this evolution, governments have drawn distinctions between differently motivated violent extremists, such as religiously-motivated violent extremism, right-wing extremism, nihilistic violent extremism, or ideologically motivated violent extremism (IMVE).³ These categories facilitate the allocation of resources for counter-terrorism professionals, while for researchers, they provide a unit of analysis from which trends and patterns can be discerned.

Analysis of terrorist activity in Canada using these categorisations leads to a disturbing realisation: IMVE is on the rise. By every measure, IMVE attacks have occurred more often and have killed and injured more people in Canada than any other type of terrorism, with the exception of the Air India attack in 1985.⁴ In response to this rise in violence, Canada has deployed one of its counter-terrorism tools: the terrorist listings process within the Criminal Code. Canada has listed several IMVE groups as terrorist entities: Aryan Strikeforce, Atomwaffen Division, The Base, Blood & Honour (and its armed wing, Combat 18), the Proud Boys, the Three Percenters, 764, the Terrorgram Collective, and Maniac Murder Cult.⁵

Beyond these listed entities, IMVE in Canada is often the purview of lone actors, individuals inspired by broader narratives but not connected to or financed by organised groups.⁶ In fact, much of IMVE activity involves individuals loosely aligned with movements rather than members of organised groups. These movements are characterised by a large number of “fellow travellers” — people who share ideas, tactics, techniques, and procedures, and encourage action among themselves, but cannot be directly tied to any specific attack or incident.⁷ A prominent example of this is the Involuntary Celibate (Incel) movement.⁸ The landscape of IMVE actors in Canada also includes semi-organised domestic IMVE networks, and Canadians are part of transnational IMVE networks, such as Active Clubs.⁹ These individuals are part of the broader IMVE movement but often support specific cells financially.¹⁰

Regardless of whether they are part of organised groups or adherents to more loosely organised movements, IMVE terrorism is perpetrated by individuals, and those individuals require funds. Those funds are used for operational financing: to acquire weapons and equipment, conduct attacks, disseminate propaganda, and organise training and events.¹¹ Additionally, organisational financing is required for terrorist organisations and movements to sustain themselves, including to pay salaries and fund propaganda creation.¹² However, post-9/11 counter-terrorist financing (CTF) policies and practices were largely designed to target organised groups such as al-Qaeda. These CTF regimes often focus on monitoring cross-border transactions and tracing financial tradecraft used by threat actors. As this article will explore, these transaction patterns and methods do not necessarily apply to IMVE actors. The question remains: which, if any, of those CTF tools are appropriate for combating the IMVE threat.¹³

This article will examine how IMVE groups, attacks, and networks in Canada are financed, using open-source reports, official publications, and completed access-to-information requests regarding the actors and incidents. By analysing seven groups, eleven attacks, and considering transnational networks, the authors aim to establish a baseline understanding of how groups in Canada raise, use, store, move, obscure, and manage funds, as well as the costs associated with IMVE attacks. Following this analysis, the article will provide an overview of the available CTF tools and evaluate their relative utility in addressing IMVE threats. The authors argue that although military approaches are unlikely to be effective (nor lawful, in most instances), states and non-state actors can employ other CTF methods to combat IMVE financing, including

leveraging financial intelligence, sanctions, and financial deplatforming. Overall, this article aims to connect the empirical data on IMVE financing in Canada to the broader CTF toolkit and examine the conditions under which different tools could be effective.

Key Concepts and Literature

The concept of *IMVE* is not widely used outside of Canada and the Five-Eyes intelligence alliance.¹⁴ Violent extremism is instead used as an umbrella term, further distinguished into right-wing extremism or left-wing extremism (which often encompasses the various types of IMVE) and jihadism.¹⁵ American institutions have also used *racially and ethnically motivated violent extremism* (REMVE), but it fails to include terrorist motivations related to anti-government sentiments or eco-terrorism.¹⁶ International institutions that shape national policy and practice, such as the Financial Action Task Force (FATF) and United Nations Office on Drugs and Crime, use terminology such as *ethnically or racially motivated terrorism* (EoRMT) or terrorism on the basis of *xenophobia, racism, and other forms of intolerance, or in the name of religion or belief* (XRIRB).¹⁷ The authors chose to maintain the IMVE terminology because the unit of analysis is Canada. Furthermore, because the IMVE concept is broad, it allows for the inclusion of left-wing violence as well as other forms of ideologically motivated violence, which are often neglected in research.

Studies into the various types of IMVE have primarily focused on intent and ideology, pathways to radicalisation, and the role of digital platforms.¹⁸ They emphasise specific groups/movements such as anti-government extremism and incels, while some ideologies, such as contemporary left-wing extremism, as well as non-American cases, receive less attention.¹⁹ There is particularly limited research on Canadian left-wing extremism, with most studies focusing on the Front de Liberation du Québec and the October Crisis of the 1960s and 1970s. Only one examination involved investigating radical environmental and animal rights groups between 1982 and 2008.²⁰

As terrorist threats have expanded beyond jihadism and ethno-nationalist terrorism, there is a growing body of research dedicated to IMVE financing. This literature has mainly examined the financing of right-wing violence, highlighting the different ways that organised entities and lone actors raise and use funds – especially in the US.²¹ Other work has examined how different crimes can be related to ideological beliefs.²² For instance, Kerodal et al. found that conspiratorial, anti-government, and anti-tax beliefs increased the risk of financial crimes such as tax evasion, while xenophobic, survivalist, and anti-gun control beliefs correlate with violent crime.²³ Reimer and Redhead analysed ideologically-motivated extremists (specifically right-wing extremists) as part of their study on self-activating terrorism.²⁴ Reports by FATF and the UNODC detail various fundraising techniques employed by EoRMT/XRIRB actors and discuss how states can prevent or respond to financing threats originating from these forms of violent extremism.²⁵ Additionally, the use of new technologies by all types of extremists has also been analysed, especially the adoption of cryptocurrencies, crowdfunding, online monetisation, and the Dark Web.²⁶ However, the IMVE financing literature does not integrate a tri-level analysis of actors, attacks, and networks.

Very few studies or policy documents have explicitly analysed CTF frameworks through an IMVE lens. A CTF framework includes eight main components: the criminalisation of terrorist financing, using financial intelligence and financial surveillance, kinetic CTF, financial exclusion (sanctions, asset forfeiture and seizure), regulatory tools, technical assistance, civil law, and financial deplatforming.²⁷ These tools and policies, which are technically threat-agnostic, have

been and continue to be applied to the IMVE threat, despite fairly significant differences in threat structure, methodologies, targets, and techniques. For instance, recent FATF work on terrorist financing has included an analysis of EoRMT financing, although little analysis has been done to examine the appropriateness of the framework for the threat.²⁸

In examining each component of the framework, the criminalisation of terrorist financing builds on the UN *Convention for the Suppression of Terrorist Financing*, FATF recommendations, and ultimately national legislation criminalising terrorist financing.²⁹ Financial intelligence is used by states to generate counter-terrorism leads by reporting suspicious activity, providing financial and account information to assist investigations, and detecting how terrorist groups, cells, and individuals finance their activities, including procurement networks.³⁰ Additionally, states use kinetic CTF measures like military action, including capture-or-kill missions, to target and dismantle terrorist financiers, cash storage sites, and sources of terrorist funding such as oil refineries.³¹ They can also interdict illicit or licit products used for terrorist financing.³² Sanctions, asset freezing and seizure, and measures to suppress the raising and movement of funds further contribute to efforts to disrupt terrorist recruitment, camps, and safe havens.³³ States also provide technical assistance to enable less-compliant jurisdictions to implement CTF standards and practices, especially criminalisation strategies.³⁴

Other actors, including the private sector, are also engaged in the fight against terrorism financing by identifying suspicious transactions and filing mandatory threshold reports.³⁵ Private sector entities further implement targeted financial sanctions and other efforts to block terrorist transactions.³⁶ The public is also involved in CTF through civil law tools that allow private individuals, namely victims of terrorism or their families, to sue terrorists and their facilitators, thus reducing terrorists' ability to fund attacks, and by extension, disrupting terrorist actors.³⁷ Finally, and most relevant to the IMVE threat, state and non-state CTF actors have sought to financially deplatform extremists by using platform terms of service to stop these entities' crowdfunding, streaming, and other efforts.³⁸

This CTF framework is being adapted here as an analytic tool to evaluate counter-IMVE financing efforts. By examining several group and attack case studies, as well as discussing transnational network financing, this article analyses how IMVE is financed and whether CTF tools work to prevent and disrupt its financing in Canada.

Methodology

To conduct the tri-level analysis of IMVE groups, attacks, and networks in Canada, the authors employed a case study protocol for each level, outlining the research methods to be used, keywords to be searched, a planned structure for analysis and reporting, as well as key themes and variables to examine. The majority of case studies were created by the first author and validated by the second author; although in some instances, outside researchers were engaged, and their findings validated by the authors. To create the case studies, the authors conducted a literature review of publicly available sources, including official documents, terrorist listing data, press releases, access-to-information requests, and parliamentary committee reviews (especially those related to the 2022 Freedom Convoy in Ottawa).³⁹ Data was also collected from news articles, court records accessed via the Canadian Legal Information Institute database, and profiles by non-governmental organisations (NGOs) such as the Canadian Anti-Hate Network. These sources were evaluated for reliability, with official sources prioritised, followed by those from dependable news outlets such as the CBC and reputable NGOs. The data was principally collected by a primary researcher (the first author) and validated by the second researcher. The

authors also cross-validated the data across several sources; however, they remained cautious of the potential of circular reporting. When discrepancies arose, such as differing accounts of weapon types, the authors used the most recent and authoritative sources, paying attention to publication history and source transparency. An abductive approach guided data collection: the authors were open to new insights while reviewing reports, but this was complemented by targeted searches for indicators common in terrorism financing, such as cryptocurrency use and other financial keywords.

The groups selected for examination are IMVE organisations listed in Canada as terrorist entities,⁴⁰ excluding the Russian Imperial Movement, as there is no evidence of this group operating in Canada, and James Mason (the author of the neo-Nazi book, “Siege”), as he is an individual, also with no known financing ties to Canada.⁴¹ This resulted in a sample of seven groups for analysis. As a result of the increased media and policy attention on incidents such as the January 6th insurrection on the US Capitol as well as the 2022 Freedom Convoy in Ottawa, there was increased attention on IMVE groups both in the US and Canada.⁴² The increased data availability led to the groups’ activities being studied beginning in February 2022, with the authors concluding data collection and analysis in October 2025. To understand how these groups (or, in some cases, movements) were financed, searches were conducted by inputting terms such as the group/network name or key associated individuals into a search engine and then within the webpages or reports, finding terms related to financing such as cash, fundraising, weapons, and others to collect information on how funds were raised, used, moved, stored, managed, and obscured in Canada, and in some cases, abroad.

Table 1: Groups Selected for Analysis

Groups
Aryan Strikeforce
Atomwaffen Division
The Base
Blood & Honour
Combat 18 (Blood & Honour's Combat Wing)
The Three Percenters
Proud Boys

In contrast to group selection, which was informed by Canadian terrorist listings, many additional factors influenced the authors’ decisions on which attacks to analyse, given the complexity of classifying and categorising violent incidents. What constitutes a terrorist attack in Canada involves several key elements. As per the Criminal Code, terrorist incidents are carried out, in whole or in part for a political, religious or ideological purpose, objective or cause, with the aim of intimidating a segment of the public and intentionally causing death or bodily harm through violence, endangering a person’s life, or posing a serious risk to the health and safety of any segment of the public.⁴³ The selection of attacks for examination was based on this definition, with a few caveats.

As it pertains to the purpose clause, determining the motivation for an incident and whether it was intended to intimidate a segment of the public is difficult, as this requires understanding the motivation of a perpetrator who often died during the course of the attack and left no detailed description of their motivation. The authors only included attacks where the perpetrator explicitly mentioned an ideological tenet. The included attacks were driven by a

variety of sentiments, such as anti-authority or anti-government extremism, incel extremism, race-motivated extremism (including neo-Nazism), and left-wing extremism. This decision on explicit mention resulted in some attacks being excluded from analysis, despite targets that might suggest an IMVE motivation.

Although attacks targeting only facilities or infrastructure would technically fall within the *Criminal Code* definition of terrorist activity, the authors chose not to include instances that caused only property damage, such as arson of religious institutions, police cars, or pipeline infrastructure. Instead, the authors focused on instances that resulted in injury or death to an individual. This approach omitted some left-wing extremist incidents, as groups like the Animal Liberation Front are primarily connected to arson or vandalism incidents, rather than violence. Because the concept of “serious property damage” is not defined in the *Criminal Code*, and few terrorism convictions address it explicitly, it was excluded due to a lack of definitional clarity. Again, this likely resulted in the exclusion of several terrorist attacks from this analysis.

Finally, while studying terrorism plots is an important methodological component of terrorism studies, terrorist plots were not included in the dataset, as this would have introduced considerable speculation into the cost estimates, given the limited available information on some disrupted plots in Canada.⁴⁴

These criteria resulted in eleven terrorist attacks attributable to IMVE actors in Canada between 2010 and 2025.⁴⁵

Table 2: Attacks Selected for Analysis, including Year and Perpetrator

Attacks
2014 Moncton Shooting (Justin Bourque)
2016 Incel Stomping Attack (Sheldon Bentley)
2017 Quebec Mosque Shooting (Alexandre Bissonette)
2018 Toronto Van Attack (Alex Minassian)
2019 Incel Knife Attack (Alexander Stavropoulos)
2020 Toronto Massage Parlour Attack (Unnamed Youth)
2020 Mosque Caretaker Stabbing (Guilherme 'William' Von Neutegem)
2021 London Truck Attack (Nathaniel Veltman)
2022 Attack on Coastal GasLink Pipeline Worksite (Unnamed Anarchists)
2022 Saanich Bank Robbery (Issac and Matthew Auchterlonie)
2023 Gender Studies Class Stabbing (Geovanny Villalba-Aleman)

Not all of these attacks resulted in terrorism charges. In many cases, the perpetrator died conducting the attack, or terrorism charges were not laid in conjunction with other serious charges, such as murder.⁴⁶ Furthermore, there have been inconsistencies in how specific ideologies, like those adopted by far-right groups, have resulted in prosecutions for hate crimes in Canada, whereas religiously motivated attacks, such as those inspired by the Islamic State, have almost always been classified as terrorism.⁴⁷

During the 2010-2025 time period, 21 individuals were charged with terrorism offences (or had a peace bond applied against them to prevent them from committing a terrorism offence) for propaganda creation and other terrorist offences.⁴⁸ Only one of those involved someone who

was actually charged with perpetrating a terrorist attack in Canada (Nathaniel Veltman).⁴⁹ The other individuals were not included in this analysis because their plots were not sufficiently advanced to be considered terrorist attacks, there was insufficient information about what they were planning (common with terrorism peace bonds), or they were charged with other offences unrelated to planning a terrorist attack, such as participation in a terrorist group (propaganda creation, for instance).

On average, terrorist attacks globally cost \$35,926, but there is considerable variation between attacks and across jurisdictions.⁵⁰ Although rare, some attacks cost nothing, whereas others, such as 9/11, cost as much as \$850,000 (adjusted for inflation to 2022 dollars).⁵¹ Comparing IMVE attacks to other forms of terrorist attacks requires a standardised understanding of cost. The cost of attacks can be estimated from information on the tactics and weapons used, as well as the number of perpetrators; for instance, more perpetrators generally require more weapons. More complex attacks tend to cost more because they require acquiring more materials, conducting reconnaissance, constructing explosive devices, and maintaining cells, whereas lower-complexity attacks tend to cost less.

For each attack, the authors collected data to estimate the costs of weapons, components, ammunition, other equipment such as vehicles or tactical gear, training and travel, and operational security expenses, including burner phones. Costs were estimated by averaging prices from local vendors based on the perpetrator's and attack's geographic locations.⁵² Further comparative cost data was collected by the second author for a separate project. This method builds on previous analysis of the Toronto 18 terrorist cell.⁵³

The cost of the attack was measured on a scale of 1-5, developed through a plausibility probe evaluating the costs of 33 attacks perpetrated between 1985 and 2018. Descriptions of the cost categories are provided in Table 3.

In addition to these groups and attacks, the authors also explored extremist networks. These networks focused on individuals and movements that engaged in violence (or threats of violence) that could meet the definition of terrorism under Canadian law and primarily consisted of groups/movements within a broader white power ecosystem in Canada.⁵⁴ The selection of groups and movements was based on inductive research, which was then expanded to focus more broadly on networks.

Table 3: Description of Attack Cost Categories⁵⁵

Cost Category	Cost Category Description
0: No-cost attack	The attack had no identifiable costs
1: Very low-cost attack	Very little money was required for the attack. The entire attack likely cost less than \$1000, and costs incurred likely included the purchase of inexpensive weapons such as knives, the rental of vehicles, or the use of already-owned material.
2: Low-cost attack	The attackers incurred some costs in the preparation of the attack, possibly including weapons purchases, vehicle rentals, specialised equipment, and operational security measures such as burner cell phones. The entire attack cost between \$1000-\$5000.
3. Medium-cost attack	The attackers incurred more significant costs in preparing for and perpetrating the attack. Possible expenses include multiple weapons purchases, improvised explosive device components, and operational security measures. The entire attack cost between \$5000-\$10,000.
4. High-cost attack	The attackers incurred significant costs while planning and perpetrating the attack. Expenses may have included a safe house, multiple weapons or explosive devices, and sustenance for attackers in the lead-up to the attack. The attack likely cost between \$10,000-50,000.
5. Very high-cost attack	The attack likely cost over \$50,000, and may have involved international travel, multiple weapons/ explosive devices, operational security measures, and possible unconventional weapons materials.

Group Finances Findings

A few of the groups analysed have had several direct financing activities in Canada; these include the Proud Boys, Blood & Honour, and the Three Percenters, among others. However, this presence and associated activity, particularly since the listing of these groups as terrorist entities, as well as the attack on the US Capitol, has decreased, likely replaced by more lone actors and movement-based participation in the IMVE landscape.⁵⁶ Nevertheless, terrorist entities have undertaken fundraising in Canada, and that activity spans a variety of sectors.

Fundraising for the listed groups has primarily taken the form of event fees, merchandise and propaganda sales, donations, membership fees, and other self-funding mechanisms.⁵⁷ Some of these groups have raised funds through criminal activity, such as drug smuggling and weapons

trafficking.⁵⁸ They have also received money for providing “security” services and for hosting concerts.⁵⁹ Funds have been further raised through donations on crowdfunding platforms and from group leaders.⁶⁰ In the US, some of these groups, such as the Three Percenters, have established charitable organisations, but similar activity has not been observed among these entities in Canada.⁶¹

IMVE groups in Canada have used these funds for propaganda, merchandise, and events.⁶² Many of them have purchased weapons and bomb-making materials, while Blood & Honour and The Base have further used funds to purchase land in the US.⁶³ Money has also been used to provide training to members, either in advance of attacks or as part of their general preparation for race wars, the collapse of society, or confrontations with police or protesters.⁶⁴ Groups have spent resources on medical expenses and legal fees for members, as well as on maintaining safe houses, websites, and even hiring individuals to serve as training or recruitment coordinators.⁶⁵ Lastly, there have been allegations that group leaders, specifically in the US, have used funds for personal purposes.⁶⁶ This is common; despite appearing strongly ideological and committed to the cause, terrorist leaders frequently divert funds for their own personal benefit.⁶⁷

Trends in the broader financial system largely determine how IMVE groups in Canada store and move funds. They have deposited money in financial institution accounts, as well as kept cash reserves.⁶⁸ However, in Canada, there is little indication of significant fund storage by these groups; instead, most of this activity is likely isolated or was undertaken for a specific purpose (such as preparation for an event). To move funds, they use cheques, cash, bank transfers, and email money transfers.⁶⁹ They have also moved money through payment processors, often as part of merchandise purchases or donations.⁷⁰

Until recently, these groups operated with impunity in Canada due to a lack of criminal listing and law enforcement attention. IMVE groups, therefore, rarely employ sophisticated financial tradecraft to conceal the source and destination of their funds. Any efforts they make to obscure their transactions are often basic and are likely by-products of other requirements (such as speed). In some cases, these groups restrict information about how to contact them and send them money, requiring prospective members to email them directly to obtain details.⁷¹ In other cases, efforts to obscure their funds are primarily driven by how the funds were acquired: when criminal activity is used to raise funds for these groups, basic money laundering techniques are sometimes employed, such as purchasing prepaid gift cards.⁷²

The use of cryptocurrencies, such as Monero, Bitcoin, and Tether by terrorist groups, including IMVE actors, has increased dramatically over the last few years.⁷³ The Base, for example, allegedly received over \$25,000 in cryptocurrency donations and schemes in the US.⁷⁴ Beyond operational security, there are ideological reasons for this: some IMVE actors seek to hasten society’s collapse or view it as imminent, and cryptocurrencies are either implicated in this downfall or seen as surviving it.⁷⁵ Some actors see cryptocurrency use as a political statement, as “it is an alternative to the traditional banks that are widely believed to be controlled by an elaborate Jewish conspiracy”.⁷⁶ The adoption and promotion of cryptocurrencies by many far-right influencers (including for personal gain, as part of a “pump and dump,”⁷⁷ scheme or “rug pulls,”⁷⁸) has also likely increased the popularity of cryptocurrencies among IMVE actors. However, this adoption is not universal: in the US, for instance, the 2022 Buffalo shooter specifically noted in his manifesto that cryptocurrencies were fundamentally “worthless” for his purposes.⁷⁹

Most IMVE groups have managed their funds in a decentralised, non-hierarchical manner, although some have employed a cell structure.⁸⁰ However, evidence of widespread fund

management techniques among IMVE groups in Canada is limited, likely due to the scattered, small-scale nature of their activities in the country. In the US, the situation has been different, with several IMVE groups, such as the Three Percenters and the Oath Keepers, establishing formal management structures, even registering charitable or not-for-profit entities.⁸¹

The lack of structure in these groups in Canada means they have never required substantial financial infrastructure. Instead, their activities and operations have been opportunistic and ad hoc. These groups share ideology and propaganda that drive terrorist attacks; yet they eschew more formal structures. This might be deliberate: these groups might be adapting to CTF efforts established after the terrorist attacks of September 11, 2001. Awareness of anti-money laundering, and CTF policies and practices, might have convinced them that establishing a large, well-financed organisation is counter-productive to their broader objectives.

Ultimately, the IMVE groups listed in Canada use a variety of means to raise funds, most of which rely on self-financing and are legal. Much of their financial activity mimics regular transactions and is often small-scale. Many of these transactions are not reported to Canada's financial intelligence unit, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), because they are below the threshold for reporting, or cannot be clearly tied to a specific group or ideological function (thus not meeting the threshold for suspicious transaction reporting). This makes it more challenging to detect their activities than for some terrorist groups that have larger-scale financial operations. At the same time, IMVE groups are no less dangerous, and thus there needs to be additional attention to developing detection and disruption techniques that account for these differences in the scope and scale of their behaviours.

Attack Finance Findings

According to FINTRAC, IMVE attacks in Canada have been “mostly” self-funded.⁸² However, analysis of these attacks indicates that, based on available information, they have been entirely self-funded, either through the diversion of the attacker's personal funds or, in some (rare) cases, by unwitting family members who provided a small amount of money in advance of the attack, not directly for the attack.⁸³ It is possible that FINTRAC has identified transactions suggesting outside funding, but these transactions have not been disclosed publicly. It is also plausible that FINTRAC is using non-definitive language to allow for the possibility of some outside funding. However, based on currently publicly available information, there is no evidence of outside funding for these attacks.

The funds were used almost exclusively for weapons, equipment, or vehicles in the attacks. In some of these attacks, such as the Saanich bank robbery, funds were diverted for training purposes.⁸⁴ However, in other cases, firearms training was common behaviour for the perpetrator, so it cannot be distinguished from pre-attack preparations.⁸⁵

These attacks in Canada have all been lone-actor attacks, with the exception of the Saanich bank robbery, which was conducted by brothers (a dyad).⁸⁶ Because these attacks involved only one to two individuals, managing the funds was simple and handled directly by the perpetrators, with no need to store or move them. The perpetrators also did not need to conceal their activities: the weapons and equipment they purchased in advance of the attack were either pre-acquired or legal in Canada.⁸⁷

The simplicity of the attacks also limits identifiable costs and pre-attack indicators.⁸⁸ The purchase of ammunition immediately preceding an IMVE attack involving firearms was common.

However, since the firearms used in the attacks were almost all legally acquired, and firearms training was common among the perpetrators, this is not an indicative financial transaction unless occurring in the context of an active threat investigation, and likely in conjunction with other financial indicators. The one exception is in the case of the Moncton shooting, when the perpetrator used a financial windfall to settle debts prior to the attack, although it remains unclear whether this was directly related to his planned attack.⁸⁹ Overall, there were few indications of attack preparation and few expenses associated with the attacks.

In assigning the IMVE attacks in Canada to a cost category (see Table 3), the majority of analysed attacks were low or very low cost, with the exception of the Saanich bank robbery, which was medium cost due to the number of firearms and equipment used.⁹⁰ IMVE attacks in Canada tend to differ from other types of attacks in that they are less expensive, although this is not universally true, and there are important outliers. The Saanich case illustrates that even self-financed lone-actor (or dyad) attacks can exceed low-cost events. This is consistent with other types of terrorism and international attacks, where self-financed lone-actor attacks can range significantly from extremely low-cost incidents to very high-cost attacks, such as the Utoya attack, the Christchurch mosque attack, and the Nice truck attack.⁹¹ Put simply, just because an attack is being planned or perpetrated by a lone actor does not mean it will be simple or low-cost. However, lone actors, and IMVE lone actors in particular, are more likely to have limited financial resources and thus choose tactics that favour low cost and pre-existing resources.

Transnational Network Finance Findings

Beyond organised IMVE groups and attacks, IMVE actors, including women, donate, facilitate financial flows, and generally transact with transnational IMVE networks.⁹² According to FINTRAC, some Canadians have financially contributed to individuals associated with international IMVE groups through international electronic funds transfers (wire transfers), using money service businesses to send funds, or through international payment processing services.⁹³ These transactions are usually small, CA\$600 or less, but are sometimes part of recurring transactions that total over CA\$10,000. Some of these transfers have been “structured”, which FINTRAC says is a deliberate effort to avoid reporting requirements.⁹⁴ However, it is also plausible that the individuals sending funds simply did not have any more money to send at any given time. Analysis of these networks suggests that they are rarely “flush” with cash, and instead, tend to exist on a subsistence basis.⁹⁵ These funds were usually sent to pay membership fees, purchase merchandise and gear, and make general donations.⁹⁶ The purpose of these transactions further supports the conclusion that the amount sent in any given transaction is dictated more by the purpose of the transaction than by efforts to circumvent reporting requirements.

Some transnational networks are also involved in crowdfunding campaigns, including cryptocurrency drives.⁹⁷ However, crowdfunding platforms have enforced the removal of this content - often under their own terms of service, but sometimes at the behest of law enforcement or security services (also known as financial deplatforming). This has displaced crowdfunding activities to smaller, less moderated platforms.⁹⁸ These platforms often lack the resources to monitor and shut down IMVE activities.⁹⁹ In other cases, these smaller platforms also lack the will or legal framework to stop this activity, compounded by the fact that they often make money from this content.

Certain Canadian companies, such as Entropy, are also major platforms for IMVE financing and organising. As extremism researcher Dan Collen writes, “Entropy is a Canadian livestreaming

service and donation platform. It garnered significant recognition between 2019 and 2021 for providing a payment platform to influential extremists who had been demonetised from larger platforms, including prominent white nationalist Nick Fuentes. Today, it is used by dozens of extremist live streamers and facilitates donations from potentially thousands of users.”¹⁰⁰ Platforms like Entropy take advantage of Canadian laws, as well as differences in laws in the jurisdictions where they operate, have accounts, or are registered. This form of jurisdictional arbitrage and exploitation can make taking action against extremist content more complicated.

Furthermore, some IMVE actors involved in transnational networks also have business accounts, and in some cases, they use these accounts to send transfers to IMVE groups.¹⁰¹ These business account transactions are characterised by irregular salary payments, a lack of business-related activity (other than insurance and loan payments), and no evidence of business-related purchases. When funds are sent or received, they are often to unrelated businesses.¹⁰² These transactions (or the lack thereof) raise questions about the nature of these accounts.

Addressing the financing of networks is difficult, especially due to challenges associated with deplatforming, listing, or criminalising their transnational and often legally grey nature. Although networks significantly contribute to the IMVE landscape through activity such as propaganda creation and communication channels, there is no available evidence that these amorphous networks maintain any type of organisational envelope for assets. While there are financial flows going through these international networks, limited visibility, different laws, and variations in intelligence capabilities impede attribution to specific actors in Canada and reduce disruption opportunities.

Countering the Financing of IMVE Organisations, Attacks, and Networks

Overall, CTF tools can be applied across the violent extremist threat spectrum, although their applicability varies significantly depending on context. Some have already been employed against IMVE actors, including sanctions,¹⁰³ criminalisation, and the use of financial intelligence to track and analyse their activities.¹⁰⁴ However, many IMVE groups are not on Canada’s terrorist list, meaning they could operate with impunity in the financial sector. Other tools, such as kinetic strikes, have varying levels of utility and legality against this type of threat. The various CTF options, and their relative utility against IMVE actors, are outlined below.

Criminalising terrorist financing is a central tool for disrupting both operational and organisational support.¹⁰⁵ These offences have enabled investigations, created necessary legal authorities, and filled gaps in existing criminal law. While the same potential exists to address IMVE in Canada, the application has been uneven. Many jurisdictions rely on hate crime or hate speech provisions rather than terrorism financing offences, which limits both deterrence and the ability to intervene early.¹⁰⁶ A further gap concerns the role of extremist propaganda as a source of financing for IMVE movements. The current CTF framework was developed for more centralised and hierarchical groups, and it does not fully reflect the reality of online content creation and monetisation that sustain IMVE ecosystems. While propaganda creation constitutes terrorist activity under Canadian law,¹⁰⁷ it is unclear if financing propaganda creation, or profiting from it, would constitute terrorist financing activity in Canada. Updating legal tools to capture these evolving financing methods and transnational networks would help ensure that criminalisation applies to all forms of extremist threats. Further, the relatively small amounts of money involved in financing IMVE activity might be a deterrent to law enforcement / public prosecutors seeking terrorist financing charges against IMVE actors.

Using financial intelligence as a disruption tool for IMVE financing has merit. Financial intelligence can provide valuable insight into how groups operate, resource themselves, and sustain networks, informing operational decision-making as well as longer-term strategic assessments. A focus on financial intelligence strengthens the ability to understand and disrupt terrorism by supporting pattern-of-life reconstruction, capability assessments, and both group- and-movement-level analysis.¹⁰⁸ The same value applies to IMVE, provided that financial intelligence approaches are fully deployed. Applying these methods to extremist groups and movements would enable a clearer picture of their networks, support systems, and financial enablers. Using movement and network analysis to examine financial links would expand intelligence exploitation and provide a more accurate understanding of IMVE ecosystems.

Military approaches that rely on capturing or killing key leaders, including those who control finance, can disrupt traditional terrorist groups by removing decision-makers and destroying cash storage sites.¹⁰⁹ In conflict settings, these actions have degraded leadership, interrupted funding flows, and imposed operational costs on groups that rely on centralised command structures. Those options are far less applicable to IMVE in Canada because it is largely domestic and lacks identifiable battlefields or easily targeted hierarchies. Instead, law enforcement tools are the appropriate means to target financial facilitators: identifying money storage mechanisms, seizing and freezing assets, and using measures such as unexplained wealth orders. There is also a need to develop specific instruments to disrupt financing that flows from movement-level activities and propagandists, for example revenue from concerts, merchandise, and online monetisation that sustains IMVE ecosystems.

Designation, sanctions, and asset freezes can be powerful tools for imposing financial friction on terrorist groups and the individuals who support them.¹¹⁰ Listing regimes and targeted measures complicate access to banking services, payment systems and commercial intermediaries, and can choke off cross-border funding routes. Where applied effectively, these measures raise the cost of doing business for organised networks and create tangible obstacles to financing and sustainment. The same mechanisms can be applied to IMVE if listing and sanctioning regimes are adapted to capture movement-level actors and enablers. Options include encouraging FATF guidance to broaden the range of groups that qualify for listing, using UN Security Council Resolution 1373 as a legal basis where international links exist, or establishing domestic designation schemes that replicate the practical effects of listing.¹¹¹ Where IMVE actors have overseas connections, prioritising those linkages and working with partners to designate simultaneously can make designation and sanctions both more feasible and more effective.

Achieving measurable results against terrorist financing through mandatory reporting by the private sector to financial intelligence units has proven elusive, and this is very much the case for IMVE financing. Transaction reporting and threshold reports generate a volume of data that supports pattern analysis and downstream investigations, but these mechanisms rarely capture the small, diffuse, or novel financing methods often used to support terrorism. The same limitations apply to IMVE; mandatory reporting alone is unlikely to be a silver bullet for identifying movement-level financing and has generally been limited against IMVE actors, often confined to post-event analysis. Further inclusion of crowdfunding platforms as reporting entities under Canadian law might increase reporting,¹¹² although many platforms accessible to IMVE actors either fall outside Canadian law, or, even if they do, these platforms are unlikely to comply with reporting requirements given their small size, international presence, and profit motive.¹¹³ Improving this tool requires providing reporting entities with clearer, actionable guidance so they can surface relevant activity. Banks and other obliged entities should be provided with an ongoing analysis of IMVE typologies and indicators. These steps would

increase the likelihood that useful leads reach financial intelligence units, but policymakers should be realistic about the marginal utility of reporting improvements and pair them with targeted intelligence and investigative measures. In addition to typologies and indicators, case studies can yield promising results as they attune compliance professionals to the variation in patterns and activities of IMVE financing.

Technical assistance has helped states build the skills and knowledge needed to detect and disrupt terrorist financing, though the quality and mode of delivery have been uneven. Traditional programmes have often relied on lecture-based training with limited practical application, reducing uptake and long-term impact.¹¹⁴ These issues are equally present when considering support to counter IMVE, where practitioners require tailored skills to understand newer financing models and movement dynamics. This is further complicated by the lack of international consensus on what constitutes an IMVE terrorist group. Without officially considering an IMVE group as a listed or designated terrorist entity, states are reluctant to engage on training on this issue. However, the nature of international IMVE networks highlight the importance of cross-jurisdictional collaboration.¹¹⁵ Terrorists, regardless of their ideology, exploit jurisdictions with lax CTF controls. The more permissive the environment, the more terrorist financing can be found. As such, international collaboration, for both investigations, and consistent policy implementation, will be key to countering the financing of IMVE actors. Collaborative exchanges and sharing of lessons learned would help broaden global understanding of IMVE financing and improve collective responses.

Civil law tools, such as civil forfeiture and civil litigation, have been used to seize assets, degrade future terrorist capabilities, and provide some compensation to victims.¹¹⁶ These measures can reduce the financial base supporting group activities and deter enablers who fear financial liability. To date, however, their use in the context of IMVE has been limited, and the potential of civil law as a disruption tool remains underdeveloped. Expanding this approach for IMVE would involve identifying viable modes of civil liability for extremist actors and supporters, and creating clearer cross-walks to enable civil tools to be used more easily across jurisdictions. There is also value in pursuing non-terrorism civil claims, such as fraud or harassment, when these avenues offer a more practical route to disruption. A broader use of civil law would diversify the toolkit available to constrain IMVE financing and impose meaningful costs on individuals and networks involved in sustaining these movements.

Financial deplatforming has removed terrorist websites, disrupted online fundraising channels, and limited access to payment processors and social media tools that generate revenue.¹¹⁷ These actions reduce the ability of groups to reach audiences, solicit funds, and maintain an online presence that supports recruitment and operational sustainment. The approach works by denying access to the financial infrastructure that underpins digital propaganda and fundraising. This tool has relevance for IMVE as actors rely heavily on mainstream platforms, crowdfunding sites, and embedded payment systems to monetise content.¹¹⁸ Greater collaboration between law enforcement, security services, and online service providers can support early identification of terms of service breaches and prompt deplatforming. Strengthening regulatory approaches to ensure that extremist actors cannot profit from harmful content can also further facilitate this cooperation. However, given the preponderance of platforms, and the network power of many IMVE actors, they are often able to regroup quickly on new platforms and resume their activities. Regardless, efforts to deplatform them from the most popular platforms can limit their reach, their ability to raise funds, and, importantly, the spread of their propaganda. Constraining IMVE actors to smaller, more obscure platforms can further create target-rich environments for intelligence services seeking to infiltrate these communities.

Finally, beyond these CTF tools, IMVE actors also engage in other forms of criminal activity. Pursuing criminal charges, including fraud or other financial violations, can offer practical avenues for disruption.¹¹⁹ For example, FINTRAC's findings about the business accounts of some IMVE actors suggest that these actors are not operating successful businesses at all, but might instead be using these accounts to reduce taxes, or as fronts for other activity, creating the possibility of investigations for tax evasion.¹²⁰ Leveraging penalties associated with other crimes provides several opportunities to potentially disrupt IMVE operational and organisational financing more easily.

Countering the financing of IMVE requires adapting CTF tools to a threat that differs fundamentally from the hierarchical, externally oriented terrorist groups for which most CTF regimes were designed. Existing instruments—criminalisation, sanctions and designation, financial intelligence, asset seizure, civil law measures, and financial deplatforming—retain value against IMVE, but only when applied with a clear distinction between organisations, individual attackers, and networks or movements. Criminalisation and designation can constrain organised IMVE actors, yet uneven listing practices leave many groups able to operate with relative financial impunity, underscoring the need for more flexible domestic and international designation regimes. Financial intelligence remains essential for disrupting individual attackers and illuminating capabilities and preparation, but its utility is greatest when legal authorities permit early intervention rather than relying solely on post-event analysis. The most significant gap lies at the movement and network level, where decentralised financing through propaganda monetisation, online platforms, merchandise, and events sits awkwardly within existing CTF frameworks. Addressing this requires new legal tools that clarify liability for financing and profiting from extremist content, expand the use of civil and non-terrorism criminal measures, and enable systematic financial deplatforming. A layered, legally updated approach that targets organisations, attackers, and sustaining networks in parallel offers the most realistic path to degrading IMVE financing and limiting its capacity to adapt and endure. However, the prospects for this approach and international coordination are limited, given the lack of international consensus on this threat.

Conclusion

Over the past decade, the rise in IMVE groups and attacks in Canada has prompted discussions about how to address the threat, particularly from a resource-denial perspective. By analysing seven IMVE groups and eleven IMVE attacks, along with transnational network financial activities, we have developed a baseline understanding of how these actors in Canada raise, use, store, move, obscure and manage funds, as well as the costs of IMVE attacks. All attacks have been self-financed, with groups also raising money for merchandise, events, and training. Both groups and individual members tend to use financial tools that reflect the current landscape, rarely employing sophisticated financial tradecraft to conceal their activities. Canadians have also contributed financially to transnational IMVE networks through donations via wire transfers, crowdfunding platforms, or business accounts.

While both state and non-state actors, including reporting entities, technology companies, civil society organisations, victims using civil litigation, and private intelligence providers, have various tools at their disposal to combat terrorist financing, their use against IMVE has been inconsistent. Military approaches are less suitable, but most other CTF measures are applicable to IMVE. Canada has adopted some CTF measures to address this threat, such as listing certain groups as terrorist entities, yet these efforts are fragmented or underutilised. Many networks

and terrorist actors have not been listed, and there is no clear process for prioritisation of the listing of IMVE groups and actors by Public Safety Canada. Sanctions and asset freezes can target IMVE actors but are less effective against decentralised networks. Updating legal frameworks to address evolving financing methods would help ensure that criminalisation captures all forms of extremist activity.

Focusing on financial intelligence is essential for better understanding and disrupting IMVE funding. However, mandatory reporting by the private sector has had limited success in both CTF and IMVE contexts. Providing clearer guidance for reporting entities, enhancing opportunities for cooperation between platforms and international partners, and better technical assistance for practitioners is critical. Moreover, expanding the use of civil law tools in this area could be beneficial. Finally, pursuing criminal charges, such as weapons offences, tax evasion, or fraud, could be beneficial where IMVE actors and activities overlap. Additional research on how the outlined tools have been used, their effectiveness against illicit actors, and a comparative analysis of IMVE financial techniques across jurisdictions, would be valuable avenues for further research.

Understanding the IMVE threat and the three main threat vectors (groups, attackers, and networks) is critical. This paper makes a significant contribution by establishing a clear baseline of the IMVE financing threat in Canada at a moment when that threat is becoming more complex, networked, and internationally embedded. It moves beyond incident-driven or ideologically focused analyses by showing how IMVE actors finance themselves, how those financial activities sustain organisations, enable attackers, and bind transnational networks, and where existing CTF tools can and cannot be applied. This analysis also describes how (and under what circumstances) IMVE actors adopt cryptocurrency or digital assets, going beyond basic analyses that only indicate use to provide more detail and nuance on extremist use of cryptocurrency. In doing so, it identifies concrete options for disruption while also demonstrating the structural limits of acting at the national level against a fundamentally transnational problem. Understanding how IMVE financing operates, which tools are available to counter it, and where partnerships are essential is therefore a necessary starting point for policy and operational responses. This paper operates as an analytic tool to better understand the utility of existing CTF tools to combat the IMVE threat in Canada. While the cases examined are in the Canadian context, these findings have broader external applicability, as many states face similar threat environments and CTF framework structures. At the same time, this article articulates an unsatisfying truth: even coherent, coordinated approaches are unlikely to deliver decisive victories against IMVE networks, and outcomes will often be partial and piecemeal. Recognising these constraints is not a weakness, but a prerequisite for realistic strategies aimed at containment, degradation, and long-term risk reduction.

Elena Martynova is a Marie Skłodowska-Curie Doctoral Fellow at Metropolitan University Prague, contributing to the EU-GLOCTER project and pursuing a PhD focused on the private sector and European Union counter-terrorism. Elena previously served as a Policy Advisor for the Canadian Government and as a Senior Research Analyst for Insight Threat Intelligence

*Jessica Davis is the president of Insight Threat Intelligence, President of the Canadian Association for Intelligence and Security Studies, and the author of *Illicit Money: Financing Terrorism in the Twenty-First Century*. Dr. Davis is presently a postdoctoral fellow at the University of Calgary, researching illicit finance.*

Endnotes

- 1 Prof. Noemie Bouhana on *Fragmented Social Ecologies Understanding the Emergence of Fluid Extremism*, directed by AVERT Research Network, 2024, 1:10:49, <https://www.youtube.com/watch?v=usqi-JLrkaBw>.
- 2 Florian. Hartleb, *Lone Wolves: The New Terrorism of Right-Wing Single Actors* (Cham, 2020); Bart Schuurman and Sarah L. Carthy, "Who Commits Terrorism Alone? Comparing the Biographical Backgrounds and Radicalization Dynamics of Lone-Actor and Group-Based Terrorists," *Crime & Delinquency* 71, nos. 6–7 (2025): 2092–117, <https://doi.org/10.1177/00111287231180126>; Bart Schuurman et al., "Lone Actor Terrorist Attack Planning and Preparation: A Data-Driven Analysis," *Journal of Forensic Sciences* 63, no. 4 (2018): 1191–200, <https://doi.org/10.1111/1556-4029.13676>; Joseph Stabile, "Beyond 'Leaderless Resistance'? Toward a Typology for White Supremacist Extremist Leadership," *Studies in Conflict & Terrorism*, January 19, 2025, 1–32, <https://doi.org/10.1080/1057610X.2024.2435074>.
- 3 For instance, the Canadian Security Intelligence Service (CSIS) has distinguished between religiously motivated violent extremism (RMVE), politically motivated violent extremism (PMVE) and IMVE. When focusing specifically on IMVE, the four main ideological delineations are: anti-government or anti-authority ideology; xenophobia; gender issues; and other grievances (often unspecified or difficult to parse).
- 4 Public Safety Canada, "Remembering Air India Flight 182," June 26, 2023, <https://www.publicsafety.gc.ca/cnt/ntnl-scrtr/cntr-trrrsm/r-nd-flght-182/index-en.aspx>.
- 5 Public Safety Canada, "Currently Listed Entities," December 10, 2025, <https://www.publicsafety.gc.ca/cnt/ntnl-scrtr/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx>.
- 6 Stephen Reimer and Matthew Redhead, *A New Normal Countering the Financing of Self-Activating Terrorism in Europe*, RUSI Occasional Paper (Royal United Services Institute, 2021), https://static.rusi.org/265_op_lone_actor_0.pdf.
- 7 Mark Peffley et al., "Terrorism and Political Tolerance toward 'Fellow Travelers,'" *Journal of Conflict Resolution* 66, nos. 7–8 (2022): 1208–34, <https://doi.org/10.1177/00220027211069121>.
- 8 This movement, composed mostly of men, mainly gathers on internet forums. Participants express misogynistic views as well as celebrate attacks perpetrated by members, even when the individuals committing those attacks were previously unknown to forum users.
- 9 Global Project Against Hate & Extremism, "Active Club Chapters Growing Globally," *Global Project Against Hate and Extremism*, June 30, 2025, <https://globalextrremism.org/post/active-club-chapters-growing-globally/>.
- 10 FINTRAC, "Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC," 2020.
- 11 Colin P. Clarke, *Terrorism, Inc.: The Financing of Terrorism, Insurgency, and Irregular Warfare* (Praeger, 2015).
- 12 Jessica Davis, *Illicit Money: Financing Terrorism in the 21st Century* (Lynne Rienner Publishers, 2021).
- 13 Jessica Davis, "Understanding the Effects and Impacts of Counter-Terrorist Financing Policy and Practice," *Terrorism and Political Violence* 36, no. 1 (2024): 1–17, <https://doi.org/10.1080/09546553.2022.2083507>; Anne L. Clunan, "The Fight Against Terrorist Financing," *Political Science Quarterly* 121, no. 4 (2006): 569–96, <https://doi.org/10.1002/j.1538-165X.2006.tb00582.x>.
- 14 *SECU Appearance: Rise of IMVE in Canada: Hearing before the Standing Committee on Public Safety and National Security* (2022), <https://www.canada.ca/en/security-intelligence-service/corporate/transparency/secu-appearance.html>.
- 15 Marc-Andre Argentino et al., *Violent Extremist Innovation: A Cross-Ideological Analysis* (International Centre for the Study of Radicalization, 2021), <https://icsr.info/wp-content/uploads/2021/12/ICSR-Report-Violent-Extremist-Innovation-A-Cross%E2%80%91Ideological-Analysis.pdf>.

- 16 *Racially and Ethnically Motivated Violent Extremism: The Transnational Threat: Hearing before the Committee on Homeland Security House of Representatives*, 117–10 (2021), <https://www.congress.gov/event/117th-congress/house-event/LC66663/text>.
- 17 Financial Action Task Force, *Ethnically or Racially Motivated Terrorism Financing* (Paris, France, 2021); United Nations Office on Drugs and Crime, *Manual on Prevention of and Responses to Terrorist Attacks on the Basis of Xenophobia, Racism and Other Forms of Intolerance, or in the Name of Religion or Belief* (Vienna, 2022).
- 18 Anda Iulia Solea and Lisa Sugiura, “Mainstreaming the Blackpill: Understanding the Incel Community on TikTok,” *European Journal on Criminal Policy and Research* 29, no. 3 (2023): 311–36, <https://doi.org/10.1007/s10610-023-09559-5>.
- 19 Tore Bjørge, Tore and Kurt Braddock, “Anti-Government Extremism,” *Perspectives on Terrorism* 16, no. 6 (2022): 2–8, JSTOR; Allysa Czerwinsky, “Misogynist Incels Gone Mainstream: A Critical Review of the Current Directions in Incel-Focused Research,” *Crime, Media, Culture* 20, no. 2 (2024): 196–217, <https://doi.org/10.1177/17416590231196125>.
- 20 Honourable Jim Carr, *The Rise of Ideologically Motivated Violent Extremism in Canada*, Report of the Standing Committee on Public Safety and National Security (House of Commons, 2022); Sue-Ming Yang et al., *Eco-Terrorism and the Corresponding Legislative Efforts to Intervene and Prevent Future Attacks*, Working Paper No. 14-04 (TSAS - Canadian Network for Research on Terrorism, Security, and Society, 2014), <https://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn31897-eng.pdf>.
- 21 Bethan Johnson, *Financing Right-Wing Extremism and Terrorism*, no. 5, Briefing (Royal United Services Institute, 2020).
- 22 Brandon A. Sullivan et al., “An Examination of the American Far Right’s Anti-Tax Financial Crimes,” *Criminal Justice Review* 44, no. 4 (2019): 492–514, <https://doi.org/10.1177/0734016819839772>.
- 23 Ashmini G. Kerodal et al., “Commitment to Extremist Ideology: Using Factor Analysis to Move beyond Binary Measures of Extremism,” *Studies in Conflict & Terrorism* 39, nos. 7–8 (2016): 687–711, <https://doi.org/10.1080/1057610X.2016.1141012>.
- 24 Reimer and Redhead, *A New Normal Countering the Financing of Self-Activating Terrorism in Europe*.
- 25 Financial Action Task Force, *Ethnically or Racially Motivated Terrorism Financing*; United Nations Office on Drugs and Crime, *Manual on Prevention of and Responses to Terrorist Attacks on the Basis of Xenophobia, Racism and Other Forms of Intolerance, or in the Name of Religion or Belief*.
- 26 Stephen Reimer and Matthew Redhead, *Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks* (Royal United Services Institute, 2022), <https://rusi.org>; Ariel Bogle, *Policy Brief: Buying and Selling Extremism: New Funding Opportunities in the Right-Wing Extremist Online Ecosystem*, no. 49 (Australian Strategic Policy Institute, 2021); Victoria Kozlova, *Examining the Intersection of Incel and Crypto Bro Phenomena: A Linguistic Qualitative Study of Harmful Ideologies in Cryptocurrency-Focused Communities*, BestMasters (Springer Fachmedien Wiesbaden, 2025), <https://doi.org/10.1007/978-3-658-47662-5>; Anti-Defamation League, *ADL Crowdfunding Report: How Bigots and Extremists Collect and Use Millions in Online Donations* (2023), <https://www.adl.org/resources/report/adl-crowdfunding-report-how-bigots-and-extremists-collect-and-use-millions-online>; Doron Goldbarsht, “Dancing in the Dark: Terrorist Financing Via the Dark Web,” in *Financial Crime and the Law: Identifying and Mitigating Risks*, ed. Doron Goldbarsht and Louis de Koker (Springer Nature Switzerland, 2024), https://doi.org/10.1007/978-3-031-59543-1_7.
- 27 Jessica Davis, “Understanding the Effects and Impacts of Counter-Terrorist Financing Policy and Practice,” *Terrorism and Political Violence* 36, no. 1 (2024), <https://doi.org/10.1080/09546553.2022.2083507>.
- 28 Financial Action Task Force, *Comprehensive Update on Terrorist Financing Risks* (2025), <https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/Comprehensive-Update-on-Terrorist-Financing-Risks-2025.pdf.coredownload.inline.pdf>.
- 29 General Assembly of the United Nations, “International Convention for the Suppression of the Financing of Terrorism,” Resolution 54/109, December 9, 1999, <https://www.un.org/law/cod/finterr.htm>; Financial Action Task Force, *FATF Special Recommendations on Terrorist Financing* (2001), <https://www.fatf-gafi.org/publications/special-recommendations-on-terrorist-financing>.

www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%20IX%20Special%20Recommendations%20and%20IN%20rc.pdf.coredownload.pdf.

- 30 "Measures to Counter the Financing of Terrorism," in *Countering Terrorist Financing: The Practitioner's Point of View*, by Mark Pieth et al. (Lang, Peter, AG, Internationaler Verlag der Wissenschaften, 2012); Aurel Croissant and Daniel Barlow, "Following the Money Trail: Terrorist Financing and Government Responses in Southeast Asia¹," *Studies in Conflict & Terrorism* 30, no. 2 (2007): 139, <https://doi.org/10.1080/10576100600959721>.
- 31 David D. McKiernan et al., *Counterterrorism and Threat Finance Analysis during Wartime* (Lexington Books, 2015), 5.
- 32 Kevin Johnston et al., *Countering Violent Nonstate Actor Financing*, Research Report (RAND Corporation, 2023), 113.
- 33 Croissant and Barlow, "Following the Money Trail," 139; Thomas J. Biersteker, "Targeting Terrorist Finances: The New Challenges of Financial Market Globalisation," in *Worlds in Collision: Terror and the Future of Global Order*, ed. Booth, Ken and Timothy Dunne (Palgrave and Macmillan, 2004), 78.
- 34 Kimberley L. Thachuk, *Terrorism's Financial Lifeline: Can It Be Severed? Strategic Forum. Number 191, May 2002*: (Defense Technical Information Center, 2002), <https://doi.org/10.21236/ADA404884>.
- 35 Fabian Teichmann and Marie-Christin Falker, "Terrorist Financing via the Banking Sector," *Crime, Law and Social Change*, ahead of print, January 9, 2024, 2, <https://doi.org/10.1007/s10611-023-10133-7>.
- 36 Thomas J. Biersteker, "Targeting Terrorist Finances: The New Challenges of Financial Market Globalisation," in *Worlds in Collision: Terror and the Future of Global Order*, ed. Ken Booth and T. Dunne (Palgrave and MacMillan, 2002), 79.
- 37 Jimmy. Gurulé, *Unfunding Terror the Legal Response to the Financing of Global Terrorism* (Edward Elgar, 2008).
- 38 Jessica Davis, "What to Do about Violent Far-Right Extremism: A Counter-Financing Framework Analysis," *Insight Monitor*, January 9, 2024, <https://newsletter.insightthreatintel.com/p/countering-the-financing-of-the-violent>; Rachel Ward et al., "Canadian Website Stops Monetizing White Supremacist Content after Fifth Estate Investigation," *CBC News*, May 20, 2026, <https://www.cbc.ca/news/canada/entropy-live-shutting-down-fifth-estate-9.7201125>.
- 39 Honourable Jim Carr, *The Rise of Ideologically Motivated Violent Extremism in Canada*.
- 40 Public Safety Canada, "Currently Listed Entities."
- 41 On December 8, 2025, the Canadian government added 3 entities to the terrorist listing that fall under the IMVE category: 764, Terrorgram Collective, and Maniac Murder Cult. Due to the decentralized nature of 764 and the Terrorgram Collective, they would fall into the category of 'transnational networks' which are discussed in a latter section of this paper. Maniac Murder Cult primarily operates in Russia and Ukraine, although there is one vandalism incident in Winnipeg that is tied to a member of the group. At the time of data collection, Maniac Murder Cult was not yet prescribed and is therefore omitted from the analysis.
- 42 Jessica Davis and Elena Martynova, "Cutting Off Financing for the Next Capitol Insurrection," *The Lawfare Institute*, August 28, 2022, <https://www.lawfaremedia.org/article/cutting-financing-next-capitol-insurrection>.
- 43 Criminal Code of Canada (2021), <https://laws-lois.justice.gc.ca/eng/acts/c-46/page-14.html#doc-Cont>.
- 44 Thomas Hegghammer and Neil Ketchley, "Plots, Attacks, and the Measurement of Terrorism," *Journal of Conflict Resolution*, December 20, 2023, 00220027231221536, <https://doi.org/10.1177/00220027231221536>.
- 45 This is a different dataset span than that for collection on the groups. If the authors used the same span as the group data collection period of 2022 to 2025, it would have been too few datapoints in terms of attacks. Meanwhile, many of the groups did not exist, have significant presence, or lacked data about them prior to 2022 to have the same search span as the attacks.

- 46 Leyland Cecco, "Twin Brothers Named as Armed Robbers Killed in Canada Bank Heist," *World News, The Guardian*, July 4, 2022, <https://www.theguardian.com/world/2022/jul/04/twin-brothers-named-armed-robbers-killed-canada-bank-heist-saanich-british-columbia>; BBC News, *Toronto van Attack: Minassian Guilty of Killing 10 People*, March 3, 2021, <https://www.bbc.com/news/uk-56269095>.
- 47 Michael Nesbitt et al., "The Illusive Motive Requirement In Canada's Terrorism Offences: Defining and Distinguishing Ideology, Religion, and Politics," *SSRN Electronic Journal*, ahead of print, 2022, <https://doi.org/10.2139/ssrn.4177368>.
- 48 Michael Nesbitt and Dana Hagg, "An Empirical Study of Terrorism Prosecutions in Canada: Elucidating the Elements of the Offences," *Alberta Law Review Society* 57, no. 3 (2020).
- 49 Justin Zadorsky, "Terror Charges Laid against Nathaniel Veltman, Accused in London, Ont. Vehicle Attack," *London, CTVNews*, June 14, 2021, <https://london.ctvnews.ca/terror-charges-laid-against-nathaniel-veltman-accused-in-london-ont-vehicle-attack-1.5469106>.
- 50 Jessica Davis, "The Cost of Terrorism," *Insight Monitor*, April 7, 2021, <https://newsletter.insightthreatintel.com/p/the-cost-of-terrorism>.
- 51 Davis, *Illicit Money: Financing Terrorism in the 21st Century*.
- 52 The authors acknowledge that there is a gap in the cost estimates for weapons obtained through informal or illegal channels. Standard vendor price averaging would not be applicable in these instances, and costs for illegally obtained weapons vary drastically depending on the specific model, as well as the location and method of acquisition. Data on cost and overall tracing of illegal firearms in Canada is out-of-date or fragmented. Statistics Canada collects data on firearms crime, but do not provide estimates on pricing. The last official government report on prices paid in Canada's illegal firearms market was compiled in 2010. However, some anecdotal evidence can provide general insights on the market. For example, in 2019, a CBC article highlighted search results from a dark-web marketplace that showcased weapons on sale for \$590 - \$1450. They further report that a firearm purchased in the US for \$200-\$300 evolves into costing \$3,000 on the black-market in Canada. Due to the lack of concrete data and significant variation in estimates, the authors have chosen to not speculate on the prices of illegally obtained weapons potentially involved in the attacks.
- 53 Jessica Davis, "Financing the Toronto 18," in *Canadian Terror: Multi-Disciplinary Perspectives on the Toronto 18 Terrorism Trials*, 1st ed., vol. 44, ed. Kent Roach et al. (University of Manitoba Press, 2021), 18.
- 54 Kathleen Belew, *Bring the War Home: The White Power Movement and Paramilitary America*, Reprint edition (Harvard University Press, 2019); Dan Collen, "Mapping Canada's White Power Ecosystem," *Insight Monitor*, April 23, 2024, <https://newsletter.insightthreatintel.com/p/mapping-canadas-white-power-ecosystem>.
- 55 Adapted from Jessica Marin Davis, "Counterterrorist Financing and the Evolution and Adaptation of Terrorist Tactics" (Carleton University, 2025), <https://hdl.handle.net/20.500.14718/43582>. All costs are adjusted to 2020 US dollars for comparison purpose.
- 56 Jessica Davis and Elena Martynova, *Analysis of the Financing of January 6th: Submission to the United States House of Representatives Select Committee to Investigate the January 6th Attack on the United States Capitol* (Insight Threat Intelligence, 2022).
- 57 Elena Martynova, "Drugs, Weapons, and Aryan Strikeforce," *Insight Monitor*, March 11, 2025, <https://newsletter.insightthreatintel.com/p/drugs-weapons-and-aryan-strikeforce>; Jessica Davis, *Group Profile: Atomwaffen Division*, Insight Threat Intelligence Case Study Library (Insight Threat Intelligence, 2023); Elena Martynova, "The Base – Financing Extremism and Foreign Interference," *Insight Monitor*, June 26, 2025, <https://newsletter.insightthreatintel.com/p/the-base-financing-extremism-and>; Elena Martynova, "Blood and Honour," *Insight Monitor*, August 1, 2023, https://newsletter.insightthreatintel.com/p/blood-and-honour?utm_medium=reader2; Jessica Davis and Elena Martynova, "Financing The Three Percenters," *Insight Monitor*, September 8, 2022, https://newsletter.insightthreatintel.com/p/financing-the-three-percenters?utm_medium=reader2; Jessica Davis and Elena Martynova, "Financing the Proud Boys: Limited Budget but an Outsized Impact," *Insight Monitor*, August 23, 2022, <https://newsletter.insightthreatintel.com/p/financing-the-proud-boys-limit>.

ed?utm_medium=reader2.

- 58 United States Attorney's Office, "Middle District of Pennsylvania | Five Men Associated With The Aryan Brotherhood Indicted For Illegal Possession And Transfer Of Firearms And Conspiracy To Distribute Methamphetamine," April 28, 2017, <https://www.justice.gov/usao-mdpa/pr/five-men-associated-aryan-brotherhood-indicted-illegal-possession-and-transfer-firearms>; Southern Poverty Law Center, "Blood & Dishonour," Southern Poverty Law Center, August 4, 2018, <https://www.splcenter.org/resources/reports/blood-dishonour/>.
- 59 Tom Keatinge et al., "Fundraising for Right-Wing Extremist Movements," *The RUSI Journal* 164, no. 2 (2019): 10–23, <https://doi.org/10.1080/03071847.2019.1621479>; The Canadian Centre for Identity-Based Conflict, "Blood and Honour – CCIBC," *Anti-Racist Canada*, 2011, <https://vtism.org/tools/vtismdatabase/blood-and-honour/>; Rachel Kleinfeld, "The GOP's Militia Problem: Proud Boys, Oath Keepers and Lessons from Abroad," *Just Security*, July 6, 2022, <https://www.justsecurity.org/81898/the-gops-militia-problem-proud-boys-oath-keepers-and-lessons-from-abroad/>.
- 60 Counter Extremism Project, "Extremist Content Online: Leader of Nazi Group the Base Posts Video and the Group Requests Cryptocurrency; German-Language Pro-ISIS Group Celebrates and Encourages Attacks," Counter Extremism Project, February 25, 2025, <https://www.counterextremism.com/press/extremist-content-online-leader-nazi-group-base-posts-video-and-group-requests-cryptocurrency>; Protos Staff, "Neo-Nazi Solicits Crypto Donations to Build US-Based Team for 'Civil War,'" *Protos*, August 6, 2024, <https://protos.com/neo-nazi-solicits-crypto-donations-to-build-us-based-team-for-civil-war/>; FATE, *Ethnically or Racially Motivated Terrorism Financing* (FATE, 2021), <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Ethnically-or-rationally-motivated-terrorism-financing.pdf>; David D. Kirkpatrick et al., "Before the Capitol Riot, Calls for Cash and Talk of Revolution," U.S., *The New York Times*, January 16, 2021, <https://www.nytimes.com/2021/01/16/us/capitol-riot-funding.html>.
- 61 Jason Wilson, "Idaho Candidate for Governor Endorsed by Rightwing Militia Leader, Video Reveals," US News, *The Guardian*, June 9, 2021, <https://www.theguardian.com/us-news/2021/jun/09/janice-mcgeachin-idaho-lieutenant-governor-rightwing-militia-leader>.
- 62 Anti-Defamation League, *The Base*, January 16, 2020, <https://www.adl.org/resources/background-er/base>; Southern Poverty Law Center, "Atomwaffen Division," *Southern Poverty Law Center*, n.d., accessed February 1, 2026, <https://www.splcenter.org/resources/extremist-files/atomwaffen-division/>; Public Safety Canada, "Currently Listed Entities - Blood & Honour," December 21, 2018, <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-en.aspx#59>; Jeremy B. Merrill, "Tech Firms Profited from Far-Right Militia Content Despite Ban on 'Three Percenters,'" News, *The Markup*, January 21, 2021, <https://themarkup.org/news/2021/01/21/tech-firms-profited-from-far-right-militia-content-despite-ban-on-three-percenters>; Anti-Defamation League, *Proud Boys, Backgrounder* (2020), <https://www.adl.org/resources/backgrounder/proud-boys-0>.
- 63 Southern Poverty Law Center, "Blood & Honour," Southern Poverty Law Center, accessed June 16, 2023, <https://www.splcenter.org/fighting-hate/extremist-files/group/blood-honour>; Alexander Meleagrou-Hitchens and Edmund Standing, *Blood & Honour - Britain's Far-Right Militants* (The Centre for Social Cohesion and About Nothing British, 2010); Martynova, "The Base – Financing Extremism and Foreign Interference."
- 64 FINTRAC, "Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC."
- 65 FINTRAC, *Access to Information Release - Background and Update on the Progress and Future Direction of the Ideologically Motivated Violent Extremism (IMVE) File within FINTRAC* (2020); Protos Staff, "Neo-Nazi Solicits Crypto Donations to Build US-Based Team for 'Civil War'"; Amy Brittain and David Willman, "'A Place to Fund Hope': How Proud Boys and Other Fringe Groups Found Refuge on a Christian Fundraising Website," *Washington Post*, January 18, 2021, https://www.washingtonpost.com/investigations/a-place-to-fund-hope-how-proud-boys-and-other-fringe-groups-found-refuge-on-a-christian-fundraising-website/2021/01/18/14a536ee-574b-11eb-a08b-f1381ef3d207_story.html.
- 66 Southern Poverty Law Center, *Three Percenters*, n.d., accessed June 3, 2022, <https://www.splcenter.org/fighting-hate/extremist-files/group/three-percenters>.
- 67 Davis, *Illicit Money: Financing Terrorism in the 21st Century*, 220.

- 68 FINTRAC, *Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Activity Financing Profile* (2021).
- 69 FINTRAC, *Access to Information Release - Background and Update on the Progress and Future Direction of the Ideologically Motivated Violent Extremism (IMVE) File within FINTRAC*; FINTRAC, *Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Activity Financing Profile* (2021); Tom Keatinge et al., “Fundraising for Right-Wing Extremist Movements: How They Raise Funds and How to Counter It,” *The RUSI Journal* 164, no. 2 (2019): 10–23, <https://doi.org/10.1080/03071847.2019.1621479>.
- 70 Jessica Davis, “Proud Boys Financing Using Canadian Financial Service,” *Insight Monitor*, June 10, 2021, <https://newsletter.insightthreatintel.com/p/proud-boys-financing>; FINTRAC, *Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Activity Financing Profile* (2021).
- 71 Keatinge et al., “Fundraising for Right-Wing Extremist Movements,” 2019; Martynova, “Blood and Honour.”
- 72 Southern Poverty Law Center, “Blood & Dishonour”; John Beauge, “Purported Aryan Strikeforce Vice President Arrested; One of Six Members Indicted,” *Pennsylvania Real-Time News, Pennlive*, May 7, 2017, https://www.pennlive.com/news/2017/05/purported_aryan_strikeforce_vi.html.
- 73 Clara Jammot, “Cryptocurrency and Extremism: How Social Network Analysis Is Used to Track Extremist Cryptocurrency Donations,” *GNET*, March 24, 2025, <https://gnet-research.org/2025/03/24/cryptocurrency-and-extremism-how-social-network-analysis-is-used-to-track-extremist-cryptocurrency-donations/>; Jessica Davis, “Beyond Anecdotes: Terrorist Financing Has Moved to Crypto,” *Insight Monitor*, January 27, 2026, <https://substack.com/@insightintel/p-185090479>.
- 74 Protos Staff, “Neo-Nazi Solicits Crypto Donations to Build US-Based Team for ‘Civil War.’”
- 75 Marc-André Argentino et al., *Financing Violent Extremism: An Examination of Maligned Creativity in the Use of Financial Technologies* (ICSR, 2023), 19, <https://icsr.info/2023/04/12/financing-violent-extremism-an-examination-of-maligned-creativity-in-the-use-of-financial-technologies/>.
- 76 Ryan Scrivens et al., “Right-Wing Extremists’ Use of the Internet: Emerging Trends in the Empirical Literature,” *GNET*, September 8, 2022, <https://gnet-research.org/2022/09/08/right-wing-extremists-use-of-the-internet-emerging-trends-in-the-empirical-literature/>.
- 77 A pump and dump scheme occurs when scammers attempt to inflate a low-value cryptocurrency with false positive statements, then sell off the currencies for a profit, causing the price to crash and new investors to lose money.
- 78 A rug pull scheme occurs when scammers inflate a specific cryptocurrency to attract investment, steal funds, abandon the project and disappear. The value crashes to zero, leaving investors with worthless assets.
- 79 Jessica Davis, “Buffalo Shooting: Financing Terrorism,” Substack newsletter, *Insight Intelligence*, May 17, 2022, <https://insightintel.substack.com/p/buffalo-shooting-financing-terrorism>.
- 80 Protos Staff, “Neo-Nazi Solicits Crypto Donations to Build US-Based Team for ‘Civil War.’”
- 81 Davis and Martynova, *Analysis of the Financing of January 6th: Submission to the United States House of Representatives Select Committee to Investigate the January 6th Attack on the United States Capitol*.
- 82 FINTRAC, “Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC.”
- 83 FINTRAC, “Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC.”
- 84 Elena Martynova, “IMVE Attack: Saanich, British Columbia Bank Robbery,” *Insight Monitor*, n.d., accessed July 17, 2024, <https://newsletter.insightthreatintel.com/p/imve-attack-saanich-british-columbia>.
- 85 CBC News, “Moncton Shooting: What Weapons Did Justin Bourque Have?,” *CBC*, June 5, 2014, <https://www.cbc.ca/news/canada/moncton-shooting-justin-bourque-was-armed-with-rifle-shot->

gun-1.2666548.

- 86 Jeff Bell and Alanna Kelly, "Details of Saanich Bank Robbery Revealed: Police the Target, Not Money," *Times Colonist*, January 20, 2023, <https://www.timescolonist.com/local-news/bank-robber-brothers-were-looking-to-kill-cops-police-say-6408196>.
- 87 Rhianna Schmunk, "Brothers, Motivated by 'anti-Authority Beliefs,' Staged Saanich Bank Robbery in Effort to Kill Police: RCMP," British Columbia, *CBC News*, January 20, 2023, <https://www.cbc.ca/news/canada/british-columbia/saanich-bank-robbery-investigation-1.6720039>.
- 88 Canadian Security Intelligence Service, *Mobilization To Violence (Terrorism) Research - Key Findings* (Canadian Security Intelligence Service, 2018), <https://www.canada.ca/en/security-intelligence-service/corporate/publications/mobilization-to-violence-terrorism-research-key-findings.html>.
- 89 Assistant Commissioner Alphonse MacNeil, *Independent Review - Moncton Shooting - June 4, 2014* (Royal Canadian Mounted Police, 2015), <https://www.rcmp-grc.gc.ca/en/independent-review-moncton-shooting-june-4-2014#sec11>.
- 90 Elena Martynova, "IMVE Attack: Saanich, British Columbia Bank Robbery," *Insight Monitor*, October 5, 2023, https://newsletter.insightthreatintel.com/p/imve-attack-saanich-british-columbia?utm_medium=reader2.
- 91 Elena Martynova, "The Christchurch Attack's Financial Blueprint," *Insight Monitor*, May 11, 2023, https://newsletter.insightthreatintel.com/p/the-christchurch-attacks-financial?utm_medium=reader2; Elena Martynova, "The Cost of the 2011 Norway Attacks," *Insight Monitor*, February 8, 2024, https://newsletter.insightthreatintel.com/p/the-cost-of-the-2011-norway-attacks?utm_medium=reader2.
- 92 Ben Makuch and Mack Lamoureux, "Unmasking 'Dark Foreigner': The Artist Who Fueled a Neo-Nazi Terror Movement," *VICE*, July 8, 2021, <https://www.vice.com/en/article/unmasking-dark-foreigner-the-artist-who-fuelled-a-neo-nazi-terror-movement/>; FINTRAC, "Access to Information Request IMVE File," 2025.
- 93 FINTRAC, "Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC."
- 94 FINTRAC, "Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC."
- 95 Jessica Davis, "Financing Incel-Motivated Terrorism," Substack newsletter, *Insight Intelligence*, May 25, 2021, <https://newsletter.insightthreatintel.com/p/financing-incel-terrorism>; Jessica Davis, "Neo-Nazis Take a Loss on Propaganda Sales," Substack newsletter, *Insight Intelligence*, January 4, 2022, <https://newsletter.insightthreatintel.com/p/extremist-year-end-revenues-and-expenses>.
- 96 FINTRAC, "Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC."
- 97 Anti-Defamation League, *ADL Crowdfunding Report*; FINTRAC, *Access to Information Release - Background and Update on the Progress and Future Direction of the Ideologically Motivated Violent Extremism (IMVE) File within FINTRAC*.
- 98 FINTRAC, "Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC."
- 99 FINTRAC, *Special Bulletin on Ideologically Motivated Violent Extremism: A Terrorist Activity Financing Profile*, nos. 2021-SIRA-001 (FINTRAC, 2021), 4, <https://www.fintrac-canafe.gc.ca/intel/bulletins/imve-eng.pdf>.
- 100 Dan Collen, "Entropy's Role in IMVE Financing," March 28, 2024, <https://substack.com/home/post/p-142650024>.
- 101 FINTRAC, "Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC."
- 102 FINTRAC, "Access to Information Act Release - Background and Update on the Progress and Future

- Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC.”
- 103 The listing of terrorist entities in Canada is considered a sanction.
- 104 Davis, “Understanding the Effects and Impacts of Counter-Terrorist Financing Policy and Practice,” 2024.
- 105 Financial Action Task Force, *FATF Guidance - Criminalising Terrorist Financing (Recommendation 5)* (2016).
- 106 Nesbitt et al., “The Illusive Motive Requirement In Canada’s Terrorism Offences.”
- 107 Royal Canadian Mounted Police Government of Canada, “Individual Associated with Atomwaffen Division Charged with Terrorism and Hate Propaganda | Royal Canadian Mounted Police,” July 5, 2023, <https://www.rcmp-grc.gc.ca/en/news/2023/individual-associated-atomwaffen-division-charged-terrorism-and-hate-propaganda>.
- 108 Sabrina Lando and Marilyne Landry, “Chapter 3: The Production and Use of Financial Intelligence to Counter Terrorism and Terrorist Financing,” in *Countering the Financing of Terrorism* (International Monetary Fund, 2023), <https://www.elibrary.imf.org/display/book/9798400204654/CH003.xml>.
- 109 Agencies, “‘Millions’ in Isis Cash Destroyed in Airstrike on Storage Site in Mosul,” World News, *The Guardian*, January 12, 2016, <https://www.theguardian.com/world/2016/jan/12/us-led-coalition-air-strike-destroys-islamic-state-cash-storage-site-in-mosul>.
- 110 Jessica Davis, “Consequences of Terrorist Listings in Canada,” *Insight Intelligence*, September 7, 2021, <https://insightintel.substack.com/p/consequences-of-terrorist-listings>; Jessica Davis, *Lessons Learned from Listing Violent Far-Right Extremist Groups in Canada*, Deterrence and Denial: The Impact of Sanctions and Designations on Violent Far Right Groups (The Soufan Center, 2022), 12, <https://thesoufancenter.org/wp-content/uploads/2022/07/TSC-IssueBrief-Jessica-Davis-July-2022.pdf>.
- 111 United Nations Security Council, “Resolution 1373 (2001),” September 28, 2001.
- 112 Jessica Davis, “Crowdfunding and Protest Financing: Emergency Law in Canada,” *GNET*, February 18, 2022, <https://gnet-research.org/2022/02/18/crowdfunding-and-protest-financing-emergency-law-in-canada/>; Financial Action Task Force, *Crowdfunding for Terrorism Financing* (2023), <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf>.
- 113 Sarah Cameron, “Why Crowdfunding Is a Top AML Risk for 2023,” *ComplyAdvantage*, January 18, 2023, <https://complyadvantage.com/insights/crowdfunding-a-top-aml-risk-for-2023/>; Davis, “Crowdfunding and Protest Financing”; Financial Action Task Force, *Crowdfunding for Terrorism Financing*.
- 114 Jessica Marin Davis, “Counterterrorist Financing and the Evolution and Adaptation of Terrorist Tactics” (Carleton University, 2025), <https://hdl.handle.net/20.500.14718/43582>.
- 115 FINTRAC, “Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC.”
- 116 Jeff Breinholt, *Pursuing Terrorists in US Civil Courts: The Encyclopedia of ATA Cases*, March 2024.
- 117 Anti-Defamation League Center for Technology and Society, *Fundraising for Hate: Platforms’ Revenue-Generating Opportunities*, Research Report (Anti-Defamation League (ADL), 2023), <https://www.adl.org/resources/blog/fundraising-hate-platforms-revenue-generating-opportunities>.
- 118 Jessica Davis and Dan Collen, “Nazis on Substack,” Substack newsletter, *Insight Monitor*, January 9, 2024, <https://newsletter.insightthreatintel.com/p/nazis-on-substack>; Jonathan M. Katz, “Substack Has a Nazi Problem,” *The Atlantic*, November 28, 2023, <https://www.theatlantic.com/ideas/archive/2023/11/substack-extremism-nazi-white-supremacy-newsletters/676156/>.
- 119 FINTRAC, “Access to Information Act Release - Background and Update on the Progress and Future Direction of the Ideologically-Motivated Violent Extremism (IMVE) File within FINTRAC.”
- 120 “FINTRAC ATIP Release Package IMVE Financing,” FINTRAC, September 9, 2022.

About

Perspectives on Terrorism

Established in 2007, *Perspectives on Terrorism* (PT) is a quarterly, peer-reviewed, and open-access academic journal. PT is a publication of the International Centre for Counter-Terrorism (ICCT), in partnership with the Institute of Security and Global Affairs (ISGA) at Leiden University, and the Handa Centre for the Study of Terrorism and Political Violence (CSTPV) at the University of St Andrews.

Copyright and Licensing

Perspectives on Terrorism publications are published in open access format and distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License, which permits non-commercial reuse, distribution, and reproduction in any medium, provided the original work is properly cited, the source referenced, and is not altered, transformed, or built upon in any way. Alteration or commercial use requires explicit prior authorisation from the International Centre for Counter-Terrorism and all author(s).

© 2023 ICCT

Contact

E: pt.editor@icct.nl

W: pt.icct.nl

