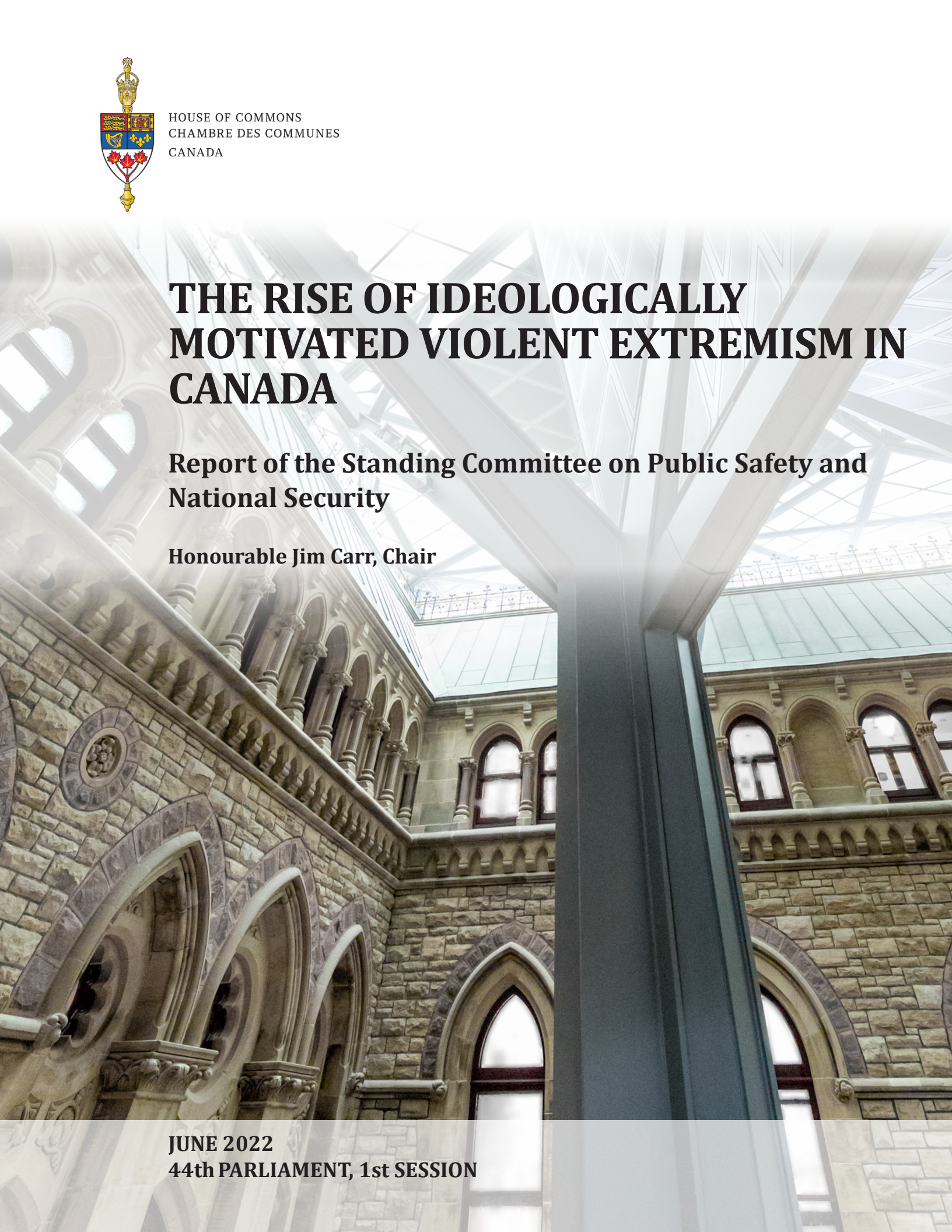

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

THE RISE OF IDEOLOGICALLY MOTIVATED VIOLENT EXTREMISM IN CANADA

Report of the Standing Committee on Public Safety and National Security

Honourable Jim Carr, Chair

JUNE 2022
44th PARLIAMENT, 1st SESSION

THE RISE OF IDEOLOGICALLY MOTIVATED VIOLENT EXTREMISM IN CANADA

Report of the Standing Committee on Public Safety and National Security

Hon. Jim Carr
Chair

JUNE 2022

44th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY

CHAIR

Hon. Jim Carr

VICE-CHAIRS

Raquel Dancho
Kristina Michaud

MEMBERS

Paul Chiang
Pam Damoff
Dane Lloyd
Alistair MacGregor
Ron McKinnon
Taleeb Noormohamed
Peter Schiefke
Doug Shipley
Tako Van Popta
Sameer Zuberi

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Vance Badawey
Kody Blois
Larry Brock
Darren Fisher
Iqwinder Gaheer
Jean-Denis Garon
Randy Hoback
Viviane Lapointe
Andréanne Larouche
Wilson Miao

Randeep Sarai
Karen Vecchio

CLERK OF THE COMMITTEE

Wassim Bouanani

LIBRARY OF PARLIAMENT

Parliamentary Information, Education and Research Services

Holly Porteous, Analyst

THE STANDING COMMITTEE ON PUBLIC SAFETY AND NATIONAL SECURITY

has the honour to present its

SIXTH REPORT

Pursuant to its mandate under Standing Order 108(2), the committee has studied the rise of ideologically motivated violent extremism in Canada and has agreed to report the following:

TABLE OF CONTENTS

LIST OF RECOMMENDATIONS 1

THE RISE OF IDEOLOGICALLY MOTIVATED VIOLENT EXTREMISM IN CANADA 9

Chapter 1: Introduction 9

Chapter 2: Defining the Threat 10

2.1 What is Ideologically Motivated Violent Extremism? 10

Chapter 3: Targets of IMVE Attacks 13

3.1 Hate Crimes 13

3.2 Under-Reporting of Hate Crimes 14

Chapter 4: Recent Trends 16

4.1 Growth and Demographics 16

4.2 COVID-19 and IMVE Narrative 18

4.3 Use of Social Media to Weaponize Conspiracy Theories and Disinformation 19

4.4 Focus on Militarization and Recruiting Military and Police Personnel 20

4.5 Financing 21

4.6 Content Presentation Algorithms 24

4.6.1 Small Online Platforms Face Special Challenges 26

Chapter 5: The Current Response to IMVE Threats 27

5.1 Terrorist Entity Listing 27

5.2 Detecting and Investigating IMVE Threats: The Importance of Data Analytics 28

5.3 Collaboration 29

5.4 RCMP Intervention Efforts 29

5.5 Public Safety Canada's Prevention Efforts 31

5.5.1 Canada Centre for Community Engagement and Prevention of Violence 31

5.5.1.1 Moonshot CVE 31
5.5.1.2 MediaSmarts 32
5.5.1.3 Centre for the Prevention of Radicalization Leading to Violence 33
5.5.2 Communities at Risk: Security Infrastructure Program 33
Chapter 6: Addressing Root Causes 34
Conclusion 36

APPENDIX A LIST OF WITNESSES 37

APPENDIX B LIST OF BRIEFS 41

REQUEST FOR GOVERNMENT RESPONSE 43

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

Recommendation 1

That the Government of Canada work with the Provinces and Territories to develop a nuanced, multi pronged, survivor-centered national strategy to address ideologically motivated violent extremism (IMVE) that includes the following elements:

Digital Safety

Recommendation 2

That the Government of Canada study the feasibility of a regulatory structure to hold platforms accountable for enforcing their terms of service, with measurable metrics to monitor that those standards are being enforced, and which could include the creation of a Digital Safety Commissioner.

Recommendation 3

That the Government of Canada work with domestic and international partners to identify and remove online bots amplifying extremist content and encourage online platforms to provide contributor and content authentication mechanisms—including web of trust style tools—that enable users to filter content on that basis.

Recommendation 4

That the Government of Canada work with platforms to encourage algorithmic transparency and reduce online use by terrorist entities by identifying terminology and phraseology for better content moderation decisions.

Preventative Measures

Recommendation 5

That the Government of Canada work with provinces and territories to increase funding for front-line, community-serving organizations—such as the Canada Centre for Community Engagement & Prevention of Violence—whose IMVE programming focuses on prevention through education, intervention, and behavioural health models as well as rehabilitation.

Recommendation 6

That the Government of Canada convene a summit with the provinces and territories to discuss how existing mental health and social services can better equip and educate front-line practitioners to provide intervention and behavioural health models that address violent and misogynistic movements, while promoting resiliency training.

Recommendation 7

That the Government of Canada both acknowledge and protect against the threats posed by violent extremism, including grievance-driven violent extremism, to Canada's critical infrastructure.

Human Rights-Based Authorities Modernization

Recommendation 8

The Government of Canada develop legislation using a human rights-based approach to adequately fund and modernize the authorities of Canada's security intelligence community with emphasis on the changing nature of technology and the role played by social media platforms in the evolution of violent extremism in Canada.

Recommendation 9

That the Government of Canada explore models adopted by other jurisdictions, like the UK and Australia, to implement a made-in-Canada solution to better tackle IMVE and the spread of online hate.

Terrorism Financing Laws

Recommendation 10

That the Government of Canada invest in its capacity to prosecute the financing of IMVE, while ensuring that terrorist financing laws are properly adapted to capture this threat.

Recommendation 11

That the Government of Canada conduct research on the role that crowdfunding, and cryptocurrency play in financing IMVE, while ensuring that the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has the resources and powers necessary to monitor suspicious transactions made through crowdfunding and cryptocurrency platforms.

Recommendation 12

That the Government of Canada ensure that terrorist financing laws are properly adapted to capture the rising threat posed by IMVE.

Recommendation 13

That FINTRAC continue to work with provinces and territories and police services of jurisdiction to share information in their mandate and continue to improve communication and collaboration.

Hate Crime Statistics

Recommendation 14

That the Government of Canada provide additional resources for Statistics Canada to train and work with law enforcement agencies to ensure that hate crime data—on which Statistics Canada should report annually—is consistently collected and comprehesive.

Addressing Biases within Military/Law Enforcement

Recommendation 15

That the Government of Canada fund research to investigate how extremist organizations are attempting to recruit individuals within the military and police services.

Recommendation 16

That the Government of Canada strengthen the internal mechanisms of the Canadian Armed Forces and federal law enforcement in order to hold personnel of these agencies accountable when they are found to be supporting violent extremist movements.

Survivor-Centered Approach to Addressing IMVE

Recommendation 17

That the Government of Canada consult with the survivors of IMVE to ensure that support and response systems reflect survivors' needs.

Protection of Religious Freedom and Safety

Recommendation 18

That the Government of Canada establish a domestically-focused counterpart to Global Affairs Canada's Office of Human Rights, Freedoms and Inclusion, ensuring that this new office is appropriately resourced and embraces a multi-faith approach in its efforts to protect and report on religious freedom and acceptance in Canada.

Recommendation 19

That the Government of Canada expand the Special Envoy on Preserving Holocaust Remembrance and Combatting Antisemitism's mandate to include more educational awareness on the Holocaust.

Recommendation 20

That the Government of Canada thoroughly reject the demonization and delegitimization of the State of Israel, and condemn all attempts by Canadian organizations, groups, or individuals, including university campus associations, to promote these views, both at home and abroad.

Recommendation 21

That the Government of Canada appoint a special envoy on Islamophobia.

Law Enforcement Training

Recommendation 22

That the Government of Canada work with the provinces and territories to develop best practices aimed at countering and investigating IMVE, hate crimes and online hate.

Recommendation 23

That the Government of Canada increase research funding to better understand and counter the operational tactics and societal impacts of all forms of IMVE—including xenophobic violence, anti-authority violence, gender-driven violence, and other grievance-driven or ideologically motivated violence.

Recommendation 24

That the Government of Canada work with the provinces and territories —in consultation with IMVE survivors— to ensure police of jurisdiction receive training on IMVE, hate crimes, and online hate, while supporting provincial police forces in their operations to infiltrate extremist circles and groups.

Law Enforcement

Recommendation 25

That the Government of Canada ensure that the RCMP, national security agencies and the Public Prosecution Service of Canada have adequate resources to investigate and prosecute offences against Canada's critical infrastructure and personnel, and ensure Canada's anti-terrorism laws are applied equally.

Recommendation 26

That the Government of Canada establish a Financial Crimes Agency and equip it with the means to investigate and identify financing of IMVE to cut off its funding at the source.

Security Infrastructure Program

Recommendation 27

The Government of Canada, in recognition of the need to address the rise in hate crimes and violence targeting religious communities and places of worship, provide increased funding for the Communities at Risk: Security Infrastructure Program and enhance it to be more effective, accessible, and responsive to community needs, including through expanded eligibility criteria and a simplified application process.

Recommendation 28

That the Government of Canada remove the need to demonstrate risk for applicants to apply to the Communities at Risk: Security Infrastructure Program and create a fast track for communities at greatest risk.

Recommendation 29

That the Government of Canada improve the Communities at Risk: Security Infrastructure Program to expand the eligibility criteria to include funding for non-physical security infrastructure.

Digital Media Literacy Strategy

Recommendation 30

That the Government of Canada create a national digital media literacy strategy that funds digital literacy programs to build Canadian's critical and civic media consumption skills across the entire population, including how to identify conspiracy theories, disinformation and misinformation online.

IMVE Awareness

Recommendation 31

That the Government of Canada continue to engage with academics, law enforcement and the public to increase awareness of IMVE and promote understanding across society of the threat posed by this form of violent extremism.

Online Hate Regulation

Recommendation 32

That the Government of Canada consult with affected communities and law enforcement agencies to identify gaps in existing law and law enforcement regarding harmful online content, while upholding Charter rights.

Recommendation 33

That the Government of Canada invest in the development of Canada's cyber infrastructure, specifically to better identify and remove automated bots used to amplify extremist content accessible to Canadians online.

THE RISE OF IDEOLOGICALLY MOTIVATED VIOLENT EXTREMISM IN CANADA

CHAPTER 1: INTRODUCTION

Ideologically motivated violent extremism (IMVE) is on the rise in Canada and its affects are being experienced throughout Canadian society, including by elected officials. Indeed, in its *2021 Public Report*, the Canadian Security Intelligence Service (CSIS) said "Ideologically motivated violent extremism […] represents a societal issue requiring a whole-of-government approach."

According to CSIS, the COVID-19 pandemic has created a breeding ground for this form of violent extremism. In its public report, it states the following:

> Since the beginning of the COVID-19 pandemic, IMVE activity has been fueled by an increase in extreme anti-authority and anti-government rhetoric often rooted in the weaponization of conspiracy theories. A number of Canadian influencers and proselytizers have emerged within IMVE movements. These IMVE influencers promote misinformation and action, including violence.

It is against this background that, on 10 February 2022, the committee adopted the following motion:

> That pursuant to Standing Order 108(2), the committee undertake a study of the rise of Ideologically Motivated Violent Extremism (IMVE) in Canada; that this study include an investigation into the influence of foreign and domestic actors in funding and supporting violent extremist ideologies in Canada; that the study include the use of social media to fuel the IMVE movement; that the committee explore the impact of anonymous and foreign donations funding IMVE, including through crowdfunding sites; that the committee invite representatives from GiveSendGo to appear; that the committee further look at the role of payment processors in preventing the funding of IMVE and invite representatives from PayPal and Stripe to appear; that evidence and documentation received by the committee from upcoming appearances of representatives of GoFundMe and FINTRAC be included in this study; that this study include Canada's national security organizations and police

> involved in monitoring, countering and responding to IMVE threats; that the committee report its findings to the House; and that, pursuant to Standing Order 109, the government table a comprehensive response to the report.[1]

The committee agreed to bring forward evidence it heard on IMVE during the 43rd Parliament. Thus, over the course of 10 meetings held between 12 May 2021 and 12 May 2022, the committee heard evidence from over 40 witnesses and received four briefs. Along with evidence taken from Canadian government officials, academics, civil society organizations and private sector representatives, the committee heard the testimony of witnesses from the United States and the United Kingdom. The committee appreciates the generosity of all these witnesses in sharing their time and expertise on this important subject.[2]

Drawing on evidence heard by the committee, this report describes what is meant by IMVE, examines the targets of IMVE attacks, recent IMVE trends, Canada's current response to IMVE threats, and presents the committee's findings and recommendations to tackle this important issue.

The committee recognizes that several areas aimed at combatting IMVE are matters of shared jurisdiction and that collaboration between all levels of government and civil society is required to address this issue.

CHAPTER 2: DEFINING THE THREAT

2.1 What is Ideologically Motivated Violent Extremism?

Terrorist activities in the age of social media now take on forms that can elude the terminology and analytical frameworks long used by our law enforcement and national security agencies. To be sure, "traditional" terrorist groups whose credo, membership, command structure and tactics are known and relatively stable have not disappeared. Rather, these longstanding national security threats have been joined by a new breed of violent extremists, lone actors and leaderless movements whose alliances and espoused causes are constantly mutating. While many of these individuals may appear to be lone actors, Mubin Shaikh, a Professor of Public Safety at Seneca College and

1 House of Commons, Standing Committee on Public Safety and National Security, *Minutes of Proceedings*, 10 February 2022.

2 For further reference, see House of Commons Standing Committee on Justice, *Taking Action to End Online Hate*, Report 29, 42nd Parliament, 1st Session, June 2019.

counter-extremism specialist for the non-governmental organization Parents for Peace, observed that an individual's propensity to commit an act of violent extremism is first motivated or directed by a larger ideologically driven movement.

Recognizing the need to use terminology that accommodates the current reality, CSIS said it now refers to threats as religiously motivated violent extremism (RMVE), politically motivated violent extremism (PMVE) and ideologically motivated violent extremism (IMVE). CSIS's Assistant Director of Requirements, Timothy Hahlweg, explained that "this new terminology […] was also chosen to mirror existing domestic legislation, paragraph 2(c) of the [*Canadian Security Intelligence Service Act*, CSIS Act], and section 83.01 of the *Criminal Code*." IMVE is of particular interest to the government. Indeed, the Senior Assistant Deputy Minister of Public Safety Canada's National Security and Cyber Security Branch, Dominic Rochon described IMVE as "one of the most serious threats we are facing today."

CSIS identifies four sub-categories of IMVE: xenophobic, gender-driven, anti-authority and other personal grievance-driven violence and notes that IMVE threat actors can be motivated by more than one grievance or occupy more than one of these sub-categories or transition from one to another.

Not all instances of extremism trigger a CSIS investigation. Mr. Hahlweg used a three-tier model to describe what kinds of extremist activities CSIS is permitted to investigate. Tier 1 activities comprise "passive engagement" with online and offline violent extremist content. Though it may be abhorrent, he said, much of the online content that forms the narrative of violent extremists is Charter-protected free speech[3] and therefore the people who engage with this content fall outside CSIS's investigative mandate. Tier 2 activities see individuals transitioning from being passive content consumers to producing and disseminating extremist propaganda. Again, much of what these individuals are producing and disseminating is protected free speech and these activities cannot be investigated. Nonetheless, Mr. Hahlweg indicated that some Tier 2 activities "bleed into" Tier 3. He explained that as some Tier 2 activities show signs of transitioning to Tier 3, CSIS focuses on indicators that people are either "mobilizing to violence or potentially mobilizing to violence." These indicators include the adoption of increased operational security measures, such as moving to private chat rooms and encrypted forums.

3 See *Canadian Charter of Rights and Freedoms*, section 2(b), which identifies as fundamental rights "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication."

Even a transition to Tier 3 does not guarantee a CSIS investigation. Some activities in this tier may be better handled through a Royal Canadian Mounted Police (RCMP) intervention or criminal investigation. Sometimes Tier 3 activities constitute hate crimes rather than terrorism. Hate crimes are strictly a police matter. Mr. Hahlweg summarized what engages CSIS's mandate as follows:

> What do we require to actually investigate these threats? We need a willingness to kill or inspire others to kill; a threat of serious violence; an attempt to effect societal change, so not just a personal narrative but something bigger; and an ideological influence. Once we have those triggers, we're able to investigate these threats. We deconflict on a regular basis with our police colleagues, especially the RCMP, and then we decide who's best positioned to deal with them.

Witnesses had varied reactions to the adoption of the IMVE terminology. Shimon Koffler Fogel, President and Chief Executive Officer of Centre for Israel and Jewish Affairs, said the move away from specific to generic labels "really captures everything in a way that is far less limiting," while Mustafa Farooq, Chief Executive Officer of the National Council of Canadian Muslims, commented that there are both beneficial and problematic aspects of adopting an "all-encompassing term" like IMVE. Former CSIS intelligence analyst, Phil Gurski, said the IMVE label is being applied to activities that may be problematic or illegal but which do not constitute terrorism as defined by the *Criminal Code*.

Neither was it clear that the academics who provided testimony for this study were fully comfortable in using this new terminology, as they often referred to the "far right" or the "far-right ecosystem"—expressions that Mr. Rochon from Public Safety Canada said the new concepts of RMVE, PMVE and IMVE were supposed to eliminate.

Christian Leuprecht, a professor at the Royal Military College and Queen's University, expressed concern about the IMVE label leading to the confounding of extremist thought with extremist violence, saying "[w]e need to distinguish between ideologically motivated violent extremism and ideologically motivated extremist violence. The former concerns the narrative, the latter concerns action." The challenge, of course, is in correctly identifying exactly when an individual has decided to act upon a violent narrative and preventing this outcome.

Perhaps what is most useful about the IMVE label is that it is agnostic to race, religion or ideology. It instead permits CSIS and the RCMP to focus on the essentials: behaviour and motive. In explaining how his organization addresses radicalization to violence, Louis Audet Gosselin, Scientific and Strategic Director of the Centre for the Prevention of Radicalization Leading to Violence, summed up the importance of focusing on the issue at this level. He said,

> [I]n the past, there have been very important extreme left-wing movements in Canada and elsewhere in the world, and that tomorrow there will be other movements. So we try to have a prevention framework that works for all ideologies. Radicalization is not just about one colour or one idea.

CHAPTER 3: TARGETS OF IMVE ATTACKS

The narratives IMVE influencers use to recruit and radicalize to violence draw on a long list of opposition and hatred. Witnesses identified many narrative themes, including but not limited to: anti-authority; Islamophobia, anti-Semitism, and other forms of religious intolerance; racism; misogyny; and anti-LGBTQ2SI as being key IMVE narrative themes that wax and wane according to current events and regional peculiarities. For example, Martin Geoffroy, Director of the Centre d'expertise et de formation sur les intégrismes religieux, les idéologies politiques et la radicalisation and Research Professor, said Quebec-based IMVE groups like La Meute, which prior to the Covid-19 pandemic had been weakened by factionalism, have been revitalized through their embrace of an anti-public health measures narrative.

3.1 Hate Crimes

Hateful narrative is regularly translated into action against Canadian communities. Mr. Koffler Fogel offered the following statistics for hate crimes committed against Jewish Canadians:

> In 2019, the most recent year for which Statistics Canada data are available, Jews were the most targeted religious group for police-reported hate crimes, and targets of the second-most-police-reported hate crime overall. On average, an anti-Semitic incident happens pretty much every day of the week, 365 days of the year. Comprising only less than 1% of the Canadian population, Jewish Canadians accounted for 16% of all victims of hate crimes in 2019, a trend repeated year after year.

Marvin Rotrand, national director of B'nai Brith Canada's League for Human Rights, said that in 2021 his organization recorded the highest level of anti-Semitic incidents in the 40 years it has been tracking such incidents. Of the 2,799 incidents recorded in 2021, he said, most occurred online. Mr. Rotrand indicated that his organization has seen a 100% increase in online anti-Semitic incidents since 2017.

Along with voicing support for the government's plans to table an online harms bill, Mr. Rotrand said government should update its anti-racism strategy to expand its definition of "hate," noting that "[a]ccording to Statistics Canada in 2020, 61% of all victims targeted for hate were members of religious minorities."

When he appeared before the committee on 16 June 2021, Mr. Farooq described some of the recent hate-driven horrors visited upon Muslim Canadians, saying:

> [W]hile I was preparing for this committee last night, I was also at the IIT, the Islamic Institute of Toronto, after two individuals yesterday threatened to bomb the centre after attempting to break in. We were also reaching out to a Black Muslim woman allegedly assaulted in Edmonton. We were also in conversation with the Baitul Hadi centre in Edmonton, which had a swastika drawn on it.
>
> On the evening of January 29, an armed male entered the CCIQ in Quebec. He gunned down six Muslim worshippers and injured several more in a terrorist attack targeting a masjid and the Muslims inside it. The victims were Ibrahima Barry, Azzedine Soufiane, Aboubaker Thabti, Khaled Belkacemi, Mamadou Tanou Barry and Abdelkarim Hassane. In an instance of hate and violence, their earthly presence was taken from us in what remains the worst attack on a house of worship on Canadian soil in modern history.
>
> On the evening of September 12, 2020, a man with alleged links to a white supremacist group, the O9A, walked onto the parking lot of the IMO mosque in Etobicoke and slit the throat of Mohamed-Aslim Zafis. I saw his body that night in the parking lot—even as I had met him that year handing out food to the poor in the worst of the COVID-19 epidemic.
>
> On June 7 a family was run down in London by an accused with alleged hate-based motivations. Terrorism charges have now been brought against the accused. I will read the names of the deceased into the record: Salman Afzaal and his mother, his wife Madiha Salman, and their daughter Yumna. Before leaving London, I met the young child, the sole survivor of the attack. I don't really have words to fully describe what that meant.

Other witnesses reminded the committee that IMVE attacks also target victims on the basis of gender. University of Ottawa law professor, Jane Bailey, said:

> [I]n terms of hateful attacks we only have to look at incel extremism in Canada and elsewhere in the world to understand the degree to which women are the subjects and objects of attack by very violent and misogynistic physical violence and rhetoric.

3.2 Under-Reporting of Hate Crimes

The committee also learned that hate crimes are under-reported in Canada. “There is no uniform way of capturing what constitutes a hate crime,” said Mr. Koffler Fogler, explaining that this under-reporting happens because “[d]ifferent jurisdictions define it differently. They have nuanced distinctions about what would fit within a category and what would not.” He observed also that police hate crime and community liaison units, are either under-resourced or non-existent in Canadian municipalities; police, Crown attorneys, and judges lack sufficient training to understand the importance of

combatting online hate; and Canada's laws to combat online harm are insufficient. Mohammed Hashim, executive director of the Canadian Race Relations Foundation, highlighted the "huge divide" between rural and urban responses to hate, saying "I think creating national standards and being able to support the small local police jurisdictions is an important intervention."

Mr. Farooq believes the problem starts with the police. He said:

> I have been in conversations with police agencies across countries, including with hate crime units, where people will call to report a hate crime and will be discouraged from reporting, or their complaint will not be taken seriously at all.

Mr. Farooq went on to describe incidents of "stalking, intimidation and trespassing" by IMVE groups such as the Soldiers of Odin where the police declined to lay charges.

According to Mr. Hashim, the perception that the police will do nothing has significant outcomes for at-risk communities. Citing a 2019 Statistics Canada general social survey in which respondents self-reported over 200,000 hate incidents, nearly half of which were violent in nature, he noted how few hate incidents come to the attention of police. Mr. Hashim said,

> Hate incidents reported to the police over the past few years represent only a fraction—probably about 1%—of that number. There is a major gap between what people are saying they're experiencing and what is actually coming to the justice system's attention. There are real impacts on individuals and communities when there is so little faith in the system, even when the system actually works.

Praising Statistics Canada's general social survey as "the best way we can measure hate crime and hate incidents in Canada," Evan Balgord, executive director of the Canadian Anti-Hate Network, recommended that these surveys be conducted annually rather than every five years.

Calgary-based imam, Navaid Aziz, offered some advice on how to ensure more hate crime is reported. He recommended that police work with community advisory boards to establish trust and facilitate communication, recognize and apologize for mistakes that have been made, hold training sessions for communities so that they better understand how to report hate crime, and, finally, remember that people who report hate crimes have been traumatized and may have difficulty in immediately recalling all the details of the event. "[T]ry your utmost not to treat them like the perpetrator, but rather treat them like the victim," he said.

Professor Bailey, argued for a Canadian IMVE strategy that extends beyond criminal law. She said criminal law's *post hoc* nature and disproportionate use against marginalized

communities, means those who are targeted by hate have good reason not to view it as a meaningful solution. Instead, she recommended "a multipronged national strategy prioritizing a survivor-centred, substantive, equality-focused approach."

In implementing such a strategy, Professor Bailey said the government should prioritize affected communities and their expertise in its policy process; focus on the responsibility that society, online platforms, and individual perpetrators have in perpetuating harms; fund trusted community agencies to serve targeted communities and an administrative body these communities can turn to in cases of tech-facilitated violence; support proactive human rights-based educational and outreach initiatives; ensure that the goal of defending the rights of members of targeted communities does not become an excuse for unnecessary expansion of police powers and surveillance; provide social context training to improve the responsiveness of the criminal justice system to survivors who turn to it; and, develop IMVE countermeasures that are tailored to specific community needs.

CHAPTER 4: RECENT TRENDS

4.1 Growth and Demographics

According to Barbara Perry, director of Ontario Tech University's Centre on Hate, Bias and Extremism, there has been "an incredible growth" in Canadian groups with far-right extremist views, with "at least 300" having emerged since 2015. However, her studies have found that the geographic concentration of these groups in Ontario, Quebec, Alberta and, to a lesser extent, British Columbia has persisted over time.

Professor Perry noted that the increased number of Canadian far-right groups reflects the "diffusion" of the far-right movement into discrete elements specifically pursuing Islamophobic, anti-immigrant, misogynistic or accelerationist agendas. She said this diffusion encourages some individuals to simply float from group to group, "cherry-picking" narratives that suit their needs.

The demographic profile of the far-right movement has also undergone recent change, said Professor Perry. While youth have always been attracted to far-right causes, she said, the movement now sees more adherents among middle-aged and older adults. It has also become more common to see members of the far right who are educated professionals earning a comfortable salary. Professor Perry called the mob that attacked the United States Capitol Building on 6 January 2021—which included a significant number of accountants, doctors and lawyers—"an inflated illustration of what we're seeing here."

Witnesses testified that there may be an imbalance of resources directed towards IMVE on different sides of the ideological spectrum. Ms. Jessica Davis of Insight Threat Intelligence remarked that there, “is a lack of application of our laws evenly across the ideological spectrum. This in the IMVE space has led to a certain sense of impunity for some of those actors.”

When asked to clarify on ‘sense of impunity’, Davis said

> In the IMVE space, there's been a real sense that a lot of these actors can get away with it, particularly because there is, to a certain extent, some radicalization in police and the military. It creates a sense that they're not going to face any consequences. I think this is true for those police officers who donated to the convoy. It might be true in some other aspects of political violence in Canada. We've been very focused on the jihadist threat for a very long time. I think we're starting to see some broadening out amongst our law enforcement security services to address other types of threats, but I'm not sure we're where we need to be yet.

Ms. Davis continued, “[in] terms of a resolution to this issue, we need to encourage resources, particularly investigative resources, to apply our laws across that political spectrum.”

During the study, Moonshot CVE, an organization dedicated to combatting IMVE gave testimony about the lack of funding they received allocated towards extremist causes traditionally associated with the left-wing of the political spectrum. Vidhya Ramalingam, co-founder of Moonshot CVE, an organization that seeks to take at-risk individuals out of IMVE spaces, commented that her organization, has “not yet done work funded by the Canadian government that looks at far-left extremism.” Ms. Ramalingam went on to say "I'm not personally aware of the full extent of programs that have been funded by Public Safety," and that "[i]n our group, specifically, work has focused on al Qaeda, Daesh, far-right extremism and incel violence." and that she, “would encourage research on far-left search activity or any far-left activity in Canada.”

Gender distribution in IMVE groups is roughly similar to that of other categories of violent extremist groups. Jessica Davis, President and Principal Consultant of Insight Threat Intelligence, estimated that female representation in Canadian IMVE groups is in the range of 15% to 30%, a figure supported by other witnesses. She noted that media coverage of these groups tends to overlook the financial and logistical work that women do, instead covering “kinetic” operations undertaken by males. Professor Geoffroy said he interviewed many women who were high-ranking members of far-right groups in Quebec and they all told him the same thing: “The role of women in this group is traditional. The women are there, ultimately, to serve the men.”

When asked about whether vaccine mandates and other measures by federal and provincial governments may have contributed to a rise in IMVE. Louis Audet Gosselin said "in some of the debates, there was a sense that those who refused to be vaccinated, especially initially, were demonized and ridiculed. This contributed to radicalization in some cases."

However, Richard Fadden, former senior national security advisor for Prime Ministers Harper and Trudeau, testified that, when identifying the root causes of IMVE, "fundamentally what drives people to this sort of thing is the sense that they are not being listened to." Mr. Fadden spoke of how the negative words and actions of senior politicians, regardless of party, directed at a given segment of the population may contribute to feelings of alienation and disenfranchisement.

On this, Tony McAleer, co-founder of U.S.-based non-profit Life After Hate, provided the following wise advice:

> People ask me what they say to their uncle or to Aunt Maggie who's spouting off all this nonsense. I ask them if they want to be right or if they want to effect change. If they want to be right, just tell Aunt Maggie all the reasons why she's wrong. If they want to effect change, listen.

Being in the minority or working at specialized roles has important implications for women who participate in the far-right movement. Aurélie Campana, Professor of Political Science at Université Laval, told the committee that she and her fellow field researchers had difficulties in persuading female members of the far right to speak to them because these women feared being recognized. Nonetheless, she said her field work showed that women are present in these groups, they are increasingly taking a public profile and, in some cases, they are serving as ideologues.

According to Vidhya Ramalingam, co-founder of Moonshot CVE, 75% of those who engage with online violent extremism content are men and violent misogyny exists across the entire spectrum of violent extremism. Nonetheless, she said women do engage with this online content and, in designing prevention mechanisms, it is important to "recognize the gender-specific interventions that are required."

4.2 COVID-19 and IMVE Narrative

Constructing narratives that echo and exploit genuine societal anxieties and grievances has been key to the expansion of IMVE in Canada. Witnesses agreed that IMVE influencers have profited from the fear and uncertainty surrounding the COVID-19 pandemic. "It's not surprising that ideologically motivated extremism grew or became

more defined during the pandemic," said Mr. Audet Gosselin. "Periods of crises are always conducive to radicalization and the emergence of extremism because they exacerbate certain vulnerability factors," he explained, adding that, during the COVID-19 pandemic, vulnerability factors such as social isolation, fear of the unknown and anxiety stemming from the pandemic caused some to adopt extreme views and solutions.

Exploiting these vulnerability factors, IMVE influencers have connected concerns over public health measures to the movement's broader corpus of conspiracy theories. "Conspiracy theories […] are used as a narrative for expressing injustice and are an articulation of fears, both real and imagined," explained Carmen Celestini a post-doctoral fellow with Simon Fraser University's The Disinformation Project. Professor Geoffroy summed it up this way: "[t]he purpose of a conspiracy theory is to find a scapegoat for our misfortunes."

Professor Leuprecht counselled against ascribing too large a role to narrative in bringing about mobilization to violence, saying "the relationship between narrative and action is indeterminate. Few in the narrative pyramid ever move to action, and action is not necessarily motivated by belief in the narrative." Ms. Celestini offered a similar view when she said "[n]ot all conspiracy theories lead to radicalization, nor do they spur political action or mobilization."

4.3 Use of Social Media to Weaponize Conspiracy Theories and Disinformation

Samuel Tanner, Professor of Criminology at Université de Montréal, described the role of social media in IMVE influence campaigns as follows:

> Social media are communications and marketing tools used by people we can call political influencers. They act in a way that shapes public opinion, not through advertising or product placement, as is done in the most traditional forms of influence, but rather by spreading doubt or a form of ready-thinking. Thus, they propose ideas or easy solutions to complex social, health or political crises and uncertainties. These ideas or solutions resonate with people who, above all, want to be reassured and have a sense of order and security.

Drawing on his own experience operating a computer-assisted hate content messaging service in 1990s, Tony McAleer made it clear that IMVE groups have long used digital capabilities to disseminate their narrative. However, with their ability to work on smartphones and enable livestreaming, social media have profoundly affected the speed and impact of these communications. As David Morin, UNESCO Chair in Prevention of

Radicalisation and Violent Extremism at the University of Sherbrooke, put it, "digital social networks and alternative media are like particle accelerators for extremism."

Social media have thus enabled what Garth Davies, associate director of Simon Fraser University's Institute on Violence, Terrorism, and Security, calls "the weaponization of conspiracy theories and disinformation." Describing a "worrying blending and metastasization of disinformation narratives and violent extremist narratives," Ms. Ramalingam said her organization had seen IMVE groups engaging in "mass movement of disinformation and conspiracy theory narratives."

Significantly, this content is not necessarily foreign in origin. According to Mr. Hahlweg, most of the abhorrent online materials CSIS encounters from IMVE groups is domestically produced. He went on to say that educating Canadians about the nature of these materials "is key." Echoing this assessment, Mr. Davies said "We must pay attention to the made-in-Canada aspects of the problem and the community-specific natures of the problem."

That said, Professor Morin expressed the view that foreign interference in the form of disinformation aimed at increasing social polarization should be a concern, saying:

> [I]t's important to point out that countries that are not interested in being nice to us, to put things prosaically, play upon the divisions that already exist in the country, and they stick a knife into an existing wound, adding noise to the noise and increasing social polarization. I think that it's essential to provide for regulatory mechanisms with more teeth, and that can—as we have seen in the Ukrainian context—monitor certain media, as has been done in Europe, and here as well. Russia Today and Sputnik are examples of propaganda media used by the Russian government.

4.4 Focus on Militarization and Recruiting Military and Police Personnel

Describing the far-right movement's "increased fascination with guns," as one of the most "dangerous" trends in IMVE, Professor Perry said that images can be found online of far-right groups posing alongside "stockpiles of weapons and engaging in paramilitary training." Noting that La Meute was founded by a former member of the Canadian Armed Forces who had been traumatized by his experience in Afghanistan, Professor Geoffroy highlighted the influence of the United States over these IMVE groups, saying:

> Right-wing extremist groups have a whole masculinity-affirming culture, and a culture that values not just freedom of expression, but also the taking up of arms, and that

> comes from the United States. The gun culture can go hand in hand with a culture that revolves around more traditional masculinity.

Mubin Shaikh, a Professor of Public Safety at Seneca College and counter-extremism specialist for the non-governmental organization Parents for Peace, had this to say about the IMVE group Diagolon:

> It's made up of former members of the Canadian Forces, individuals with real combat training, with real capabilities and who have grown increasingly radicalized, especially because of COVID. These are people with weapons. There is an alleged connection between this group and the group that was arrested at the Coutts border crossing, who were ready to engage police in a firefight, in a shootout.
>
> These are the kinds of groups that I consider to be a real and significant threat to Canadian public safety at large.

IMVE groups are intent on enhancing their capacity for violence. Professor Perry said her research on the far right's efforts to infiltrate the Canadian Armed Forces [CAF] uncovered instances of far-right group members enlisting in the CAF, often as reservists, to receive training they can share with their group. She said far-right groups also seek to recruit serving members of the military and veterans, the latter of whom may lack the kinds of social supports they had in the CAF and are "looking for a familiar place to belong."

Wendy Via, co-founder of U.S.-based Global Project Against Hate and Extremism, made the following observation:

> Canada and the United States have long had similar and intertwined white supremacist, anti-government and other hate movements. In recent years we have seen American hate and militia organizations, including the neo-Nazi The Base, the anti-government Three Percenters, the misogynistic and racist Proud Boys and others establish themselves on both sides of the border. Because these organizations attempt to infiltrate key institutions, both countries are facing the issue of extremists in the military and the police, though to varying degrees.

Ms. Via went on to recommend the creation and enforcement of strong policies against extremism in the military and police forces, from recruitment to active duty to veteran status.

4.5 Financing

To date, IMVE attacks in Canada have been conducted primarily by lone actors using minimal resources. These "self-financing, low-level, low-cost attacks" are a good

indication that Canada's counter terrorism financing policies have been "somewhat effective," said Jessica Davis.

However, a truck convoy's weeks-long occupation of Ottawa and of border crossings in Emerson, Manitoba; Coutts, Alberta; Windsor, Ontario; and, Surrey, British Colombia in early 2022 has shone a light on how quickly small groups can raise vast sums of money through U.S.-based crowdfunding platforms like GoFundMe or GiveSendGo. In this case, the convoy's organizers used crowdfunding to purchase the fuel and supplies that kept the Ottawa occupation going.

Though GoFundMe ultimately disbursed only USD$1 million of the over USD$10 million in donations raised on its platform, the fact that this staggering sum could be amassed in such a short period of time is concerning. Indeed, the volume and velocity of donations being directed to the truck convoy was so out of the ordinary that GoFundMe's President, Juan Benitez, told the committee that his company started monitoring the fundraising campaign a day after its 14 January 2022 creation. According to Mr. Benitez, 88% of donated funds originated in Canada and 86% of donors were from Canada.

GoFundMe suspended this fundraiser twice, first on 25 January 2022 and then again on 2 February 2022 to review its adherence with the company's terms of service before it finally shut it down altogether on 4 February 2022. Mr. Benitez said, "From February 2 through February 4, we heard from local authorities that what had begun as a peaceful movement had shifted into something else. They shared reports of violence and threatening behaviour by individuals associated with this movement."

Another U.S.-based crowdfunding platform, GiveSendGo, did not hesitate to offer a venue for the truck convoy's fundraising activities. On 2 February 2022, two fundraisers for the truck convoy became active on GiveSendGo's website. By 10 February 2022, when the Province of Ontario successfully petitioned the Ontario Superior Court of Justice to freeze access to these two GiveSendGo fundraisers, some USD $9 million in donations had been raised on this platform.

At the time, Barry MacKillop, the deputy director of the Financial Transactions and Reports Analysis Centre of Canada's (FINTRAC's) intelligence unit, told the committee that, because they are located in the United States, crowdfunding platforms were not subject to Canadian laws. He noted, however, that payment processors with a Canadian presence and Canadian banks that are used to transfer funds to or from these platforms were subject to the registration and reporting requirements of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA). He explained that

> As part of their obligations, businesses subject to the [PCMLTFA] are required to establish a compliance program, identify clients, keep records and report certain types of financial transactions to FINTRAC, including international electronic funds transfers totalling $10,000 or more in a 24-hour period, large virtual currency transactions totalling $10,000 or more in a 24-hour period, and suspicious transactions, which have no monetary threshold for reporting.

Nonetheless, once the federal government invoked the *Emergency Measures Act* on 14 February 2022, it immediately issued orders requiring crowdfunding platforms and foreign payment processors to keep customer records and report transactions of $1000 or more in funds or virtual currency to FINTRAC. These emergency provisions have subsequently been made permanent through new regulations issued in the *Canada Gazette* on 27 April 2022.[4]

In this regard, it is significant that on 10 February 2022—the day before the Province of Ontario declared a state of emergency—Mr. MacKillop said the following to the committee: "[w]hat's happening in Ottawa has not been, to my knowledge, identified as ideologically motivated violent extremism."[5]

Had FINTRAC generated any intelligence indicating that the truck convoy was obtaining the proceeds of crime, engaging in money laundering, or financing terrorism, it would have had a duty to disclose this intelligence to appropriate federal entities, including the RCMP and CSIS. Mr. MacKillop told the committee that "we have not seen a spike in suspicious transaction reporting" related to the Ottawa truck convoy. No suspicious transaction reporting means no FINTRAC disclosures.

Then there is the question of what actions are taken when FINTRAC does make a disclosure. Stephanie Carvin, an associate professor at Carleton University's Norman Paterson School of International Affairs, said "Canada has been largely unsuccessful in prosecuting terrorism financing charges, despite very broad and inclusive definitions of what constitutes financing." Citing Ms. Davis' work, she noted that out of 4600 FINTRAC disclosures on suspected terrorist financing activities, Canada has only successfully prosecuted 2 cases. She acknowledged, however, that there is no public information on

4 Changes to FINTRAC reporting requirements since the revocation of emergency orders suggest that, while the previous PCMLTFA regime may have ensured Canadian banks and money service businesses could respond promptly to provincial- and federal-level orders to freeze truck convoy assets after an emergency had been declared, this regime was of little use in providing warning about fundraising activities prior to the emergency.

5 As a senior official with responsibility for intelligence at FINTRAC, Mr. MacKillop would presumably have full access to any Integrated Terrorism Assessment Centre (ITAC) threat assessments concerning the truck convoy. ITAC is responsible for assessing terrorism threats to Canada and Canadian interests worldwide.

the number of threat disruption activities that may have been undertaken on the basis of these disclosures.

In respect of countering IMVE fundraising, Ms. Carvin supported the government's proposed new Financial Crimes Agency, but said "much depends on the government's willingness to develop the capacity to investigate and prosecute in this area."

Perhaps the new post-emergency reporting requirements for crowdfunding platforms and foreign money service businesses will help flag fundraising activities for large-scale IMVE events. But it is less clear how they will address the threat posed by self-financed lone actors who have been radicalized to violence or by the online IMVE influencers who are bent on inspiring others to engage in violence. Speaking about the latter, Brandon Rigato, a doctoral candidate at Carleton University specializing in right-wing and religious terrorism, said: "We can't overlook the fact that these are, often, ideologically motivated people who will do it free of cost. Some of the most vociferous posters have no funding, other than their own BitChute channels."

"Funding is not driving this," said Mr. Davies, "GoFundMe and other platforms are not driving IMVE in Canada or anywhere else."

Another witness argued that there may be value in going after other forms of support for IMVE activities mediated through online platforms. Using Uber and Airbnb as examples, Vivek Krishnamurthy, Samuelson-Glushko Professor of Law at the University of Ottawa, urged the government extend regulation of crowdfunding platforms to other platforms that can be used to facilitate IMVE activities in the physical world. He said:

> I would suggest that it would be a useful approach for Parliament to consider to extend regulation that applies in the bricks and mortar physical world to activities online, especially those that could be used to facilitate and incite online violence or violence in the real world.

4.6 Content Presentation Algorithms

There is a "big money" dimension to online IMVE activities which witnesses say has not been addressed effectively by Canada's existing regulatory framework. Imran Ahmed, Chief Executive Officer of the United Kingdom-based Center for Countering Digital Hate, told the committee that millions are being made from "spreading discord and peddling lies." He explained the business model as follows:

> The truth is that there is a web of commercial actors, from platforms to payment processes to people who provide appetizing technology that is embedded on hateful content, giving the authors of that hateful content money for every eyeball they can

> attract to it. It has revenues in the high millions, tens of millions and hundreds of millions of dollars that have made some entrepreneurs in this space extremely wealthy.

According to Mr. Ahmed, the logic is as follows: social media platforms rely on advertising revenue; advertisers make money when their advertisements appear alongside highly engaging content; and, knowing that users engage most with content that elicits strong emotions like hate and outrage, social media platforms optimize advertising opportunities through algorithms that promote polarizing content. He noted that, since its establishment in 2016, his organization has seen a broad swath of IMVE actors using online platforms to disseminate harmful content, saying

> The reason we started this organization was that we were seeing the rise of virulent anti-Semitism and disinformation on the left in the United Kingdom, as well as seeing that fringe actors, from anti-vaxxers to misogynist incels to racists such as white supremacists and jihadists, are able to easily exploit digital platforms to promote their own content.

Michele Austin, Twitter's director of public policy for the United States and Canada, said her company "has much less algorithmic content than our competitors" and that users can turn off its recommendation algorithm. She said Twitter "aggressively fights" IMVE activities on its platform and has "invested heavily in technology and tools to enforce our policies."

Officials from Meta, Facebook's owner, vigorously denied claims about the profit-driven nature of its content-promotion algorithms, saying that, while they make money from advertising, some of these profits are reinvested into enhancing safety. Rachel Curran, Meta Canada's Public Policy Manager, said her company has reinvested $13 billion into "securing the safety of our community" since 2016.

Ms. Via told the committee that, for all their assertions otherwise, large online platforms are still not investing enough in policy enforcement:

> Twitter, Facebook, YouTube—all of them have rules about what can be aired on their platforms, but it's the enforcement. It is unequally enforced. It is inadequately enforced. There is not enough staff. There's not enough cultural and language competency in order for that to happen.

In considering what it is government should do to ensure online platforms address IMVE content expeditiously, witnesses advocated for an arm's length approach. Mr. Balgord recommended the establishment of an "ombudsperson that is a well-resourced regulator with investigatory powers" extending to the examination of content presentation algorithms. This ombudsperson should be empowered to issue

recommendations, he said, and—where these recommendations are not acted upon—the ombudsperson should be able to apply for a judicial review.

Ilan Kogan, a data scientist with Klackle, highlighted the risk of "collateral censorship." "Where there's even a small possibility that speech is unlawful," he explained, "the intermediary will err on the side of caution, censoring speech, because the cost of failing to remove unlawful content is too high." Mr. Kogan recommended that Canada adopt the European Union's approach to online harms, saying:

> [T]he path forward is a focus on transparency and due process, not outcomes: independent audits; accuracy statistics; and a right to meaningful review and appeal, both for users and complainants.

4.6.1 Small Online Platforms Face Special Challenges

Adam Hadley, executive director of United Kingdom-based non-profit Tech Against Terrorism, which receives Public Safety Canada funding, told the committee that terrorists and violent extremists often use small online platforms to exploit these platforms' limited knowledge and capabilities. To address this issue, he said Tech Against Terrorism provides small platform operators free access to a knowledge-sharing platform (KSP). Explaining what the KSP offers, he said:

> [T]he KSP provides information on logos associated with designated groups, the terminology associated with them and phraseology that may be typical of the content that appears. There's also detail on workflow in order to support platforms in making better content moderation decisions. There is also a significant amount of information about designation lists at the international level and a summary of global online regulatory efforts and many other elements.

Mr. Hadley indicated that most small online platforms lack capacity or capability to develop complex automation, saying, "the automation that we typically support with is fairly simple and it's about helping them make the right decisions and record the decisions that they're making." Automation of this nature supports transparency reporting, he said, "an important principle in all content moderation." Mr. Hadley went on to recommend that "platforms of all sizes invest in transparency reporting."

University of Ottawa computer science professor, Diana Inkpen, warned the committee that, due to their inaccuracy, automated tools alone will be insufficient to identify and remove harmful online content, saying that,

> In my opinion, there will always be a need for humans in the loop, not only to use these tools with a grain of salt but also to try to get an explanation of why the machine recommends such things.

The committee agrees that, at the very least, online platforms need to do a better job of enforcing their own acceptable use policies. While it is understandable that some of the smaller and less resourced platforms may struggle to detect and remove content that violates company policies prohibiting harmful or illegal content, it is harder to fathom why, if they are truly not sacrificing the public good for profit, large and well-resourced platforms continue to fall so short of the mark. Although Meta and Twitter told the committee they invest heavily in technology and human resources to enforce their policies, the harms that arise from the shortcomings of their efforts are undeniable and there is good reason to believe that these harms will persist until the current approach is changed.[6]

CHAPTER 5: THE CURRENT RESPONSE TO IMVE THREATS

The government's current response to IMVE threats attempts to be comprehensive in addressing the entire lifecycle of radicalization to violence. Despite this, the committee heard from a number of witnesses that there is room for improvement, particularly in respect to early and preventative interventions. In the view of some witnesses, including former CSIS director and national security advisor to the Prime Minister Richard Fadden, the government relies too heavily on national security and law enforcement agencies to reduce IMVE threats when it could use existing or nascent capabilities within communities across Canada earlier and to greater effect. The following sections examine some of the key tools the government uses to confront IMVE threats.

5.1 Terrorist Entity Listing

The committee heard that terrorist entity listing under section 83.05(01) of the *Criminal Code* provides an important way for the government to reduce terrorist threats. The entity listing process has been described as "a public process for identifying, without the need for charge, trial and conviction, an entity so as to dissuade others from dealing with it."[7] From the government's perspective, the act of publicly labelling an entity as terrorist in nature has immediate and beneficial impacts. First, when an entity is listed, banks and financial institutions must immediately freeze its assets, as knowingly handling these assets has become a criminal act. Second, listing an entity informs the public about the government's stance on that entity and conveys the message that they risk criminal prosecution if they associate with or provide support for these entities.

6 SECU, *Evidence*, 5 May 2022 (Imran Ahmed, Chief Executive, Center for Countering Digital Hate), SECU, *Evidence*, 26 April 2022 (Wendy Via, Co-Founder, Global Project Against Hate and Extremism), SECU, *Evidence*, 26 April 2022 (Ilan Koga, Data Scientist, Klackle, As an Individual).

7 Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril*, p. 277.

Third, because a terrorist entity need not have conducted terrorist acts against Canada to be listed, listing an entity that has either engaged in or facilitated such acts against other countries conveys the government's commitment to its international counter-terrorism obligations.[8]

Witnesses spoke positively about the addition in 2021 of six neo-Nazi groups and one individual neo-Nazi—the Proud Boys, The Base, Russian Imperial Movement, Atomwaffen Division, Aryan Strikeforce, Three Percenters, and James Mason– to Canada's Listed Terrorist Entities. For example, Mr. Hadley praised Canada's "pioneering work in designating organizations from across the terrorism and violent extremism spectrums," saying such "designation is a crucial tool that can be used to help provide that clarity so that small tech platforms get better at dealing with terrorist activity." Nonetheless, he recommended that the government examine how its listing process could be expedited.

5.2 Detecting and Investigating IMVE Threats: The Importance of Data Analytics

Detecting and investigating IMVE threats has become an increasingly data-driven task. CSIS officials repeatedly voiced their desire to see the Service's mandate "modernized" so the Service can keep up with online IMVE threats. Noting Canada's ongoing negotiations with the United States on the latter's *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act)—which would expedite lawful access to data stored on servers outside of Canada in CLOUD Act partner countries—Cherie Hendersen, CSIS's assistant director of requirements, said "this sort of legislation could help us because it then allows us access to greater volumes of information." She indicated that two of Canada's Five Eyes intelligence allies, the United Kingdom and Australia are further advanced in their CLOUD Act negotiations with the United States.

It appears, then, that expanded authorities to access and exploit data generated through online activities is an important element of the modernization CSIS seeks. Should such expanded authorities form part of a proposed CSIS Act amendment package, Ms. Carvin suggested the following considerations for Parliament:

> [U]nder what circumstances does Parliament think that CSIS should have the power to go into online spaces to investigate violent extremist threats? Or request basic subscriber information? Should the least

8 Ibid, pp 277-287.

> intrusive means have the same requirements as the most intrusive means?

In posing the last of these questions for Parliament, she was referring to potential amendments to the CSIS Act's current section 21 requirement to obtain a Federal Court warrant whenever it seeks to intercept, obtain and retain communications, records, documents or things.

5.3 Collaboration

CSIS and the RCMP both emphasized the value they place on collaboration in monitoring and responding to IMVE threats, not only between themselves, but with other federal government stakeholders, provincial, territorial and municipal governments, and civil society organizations. "This threat is a multi-faceted problem, going well beyond law enforcement and national security," Mr. Hahlweg said, adding that IMVE "requires a whole-of-government response, engaging social, economic and security mandates." Indeed, Public Safety Canada's director general for national security policy, Lesley Soper, went one step further, characterizing IMVE as "a whole-of-society question." This call for a comprehensive approach was echoed by numerous witnesses.

For its part, the RCMP has been training its members to recognize key indicators that an IMVE group is forming or an individual has begun to embrace violent extremism. According to the head of the RCMP's Federal Policing program, Deputy Commissioner Michael Duheme, the plan is to work with the Canadian Association of Chiefs of Police so that law enforcement agencies across Canada can receive the same training in detection of IMVE threats.

5.4 RCMP Intervention Efforts

Sometimes early intervention can prevent a violent outcome. On the latter, Chief Superintendent Mark Flynn, RCMP Assistant Commissioner for Federal Policing, National Security and Protective Policing, described the RCMP's new approach to intervention as follows:

> In our protective policing program, we have behavioural scientists who review the intelligence or evidence that comes in with respect to threats and the individuals who are involved. We put those people into defined categories with defined follow-up regimes based on the levels of threat, particularly when they don't meet the criminal threshold where there's likely going to be a conviction based on their activity.

> […] It's a very highly skilled group that is developing these assessments as well as the plans to intervene. That can go anywhere from a regimented monthly follow-up with public health officials, psychological services, counselling and so on, to someone who's at the very low end of the threshold potentially having annual follow-ups to determine whether or not they are increasing or decreasing their activity. It's a very effective group, and I'm very proud of the service that they provide.

It is noteworthy that the RCMP looks to public and mental health experts to help conduct these interventions and the focus is on addressing the underlying psychological issues that have caused individuals to engage with IMVE content. While this initiative is a welcome form of early and preventative intervention, the Committee learned that there are risks in relying on a law enforcement agency to undertake this kind of work. For example, establishing the trust that is necessary to successfully conduct interventions of this nature is that much harder when police are in any way involved.[9] Moreover, by the time a person who poses an IMVE threat has come to the attention of police, it may be too late to mount an intervention that has a lasting and positive effect.[10]

On 17 February 2022, several dozen attackers with weapons ransacked the Coastal Gaslink pipeline worksite, a critical infrastructure project for Canada, causing millions of dollars in damage and terrorizing workers on-site. When asked in committee if any arrests had been made three months after the fact, officials could not confirm whether they were aware of any arrests; however, Assistant Director of CSIS, Cherie Henderson said "I can't go into the specifics of what we do in an investigation, just to ensure that we can protect our methods, but I can say that we certainly do look at these, and we use all of our investigative powers" and Deputy Commissioner Michael Duheme of the RCMP said "I can confirm that the matter is being investigated, but that would be on the provincial side because there is no element right now that would fall under the federal policing mandate."

Posing the question, "who is best suited to deal with the root causes of IMVE?", Mr. Fadden offered the following answer:

> While they may have a role, in my view at any rate, it is certainly not CSIS, the RCMP, nor police more generally. Provinces, cities and civil society will have to be involved. Perhaps the federal role should be developing a framework, coordinating and perhaps providing some funding.

9 SECU, *Evidence*, 12 May 2022 (Richard Fadden, As an Individual).

10 SECU, *Evidence*, 5 May 2022 (Tony McAleer, Author and Co-founder, Life After Hate, As an Individual).

5.5 Public Safety Canada's Prevention Efforts

5.5.1 Canada Centre for Community Engagement and Prevention of Violence

Public Safety Canada's Canada Centre for Community Engagement and Prevention of Violence (Canada Centre) leads the government's efforts to counter radicalization to violence. In practice, this means funding projects and networking activities. Through its Community Resilience Fund, the Canada Centre funds research and other activities across Canada that will "improve Canada's understanding and capacity to prevent and counter violent extremism."

The Canada Centre's work received positive commentary from some witnesses. For example, Mubin Shaikh lauded its "collaborative approach" and decision to rely on existing community-based groups and civil society to "work on the ground with at-risk communities" and deal with grievances "on a one-to-one basis." However, both he and Professor Perry called for additional resources to be directed towards those who are undertaking these efforts on behalf of government. On this matter, Professor Perry had the following to say,

> Whether it's working in partnership with boards of education or even particular teachers to develop curricula, or whether it is developing programs that might be offered in the community through partnerships with other community groups, for me, the key is enhancing the capacity of community-based organizations with expertise in this area.

Tech Against Terrorism, Moonshot CVE, MediaSmarts, and the Centre for the Prevention of Radicalization Leading to Violence are all initiatives that have received support from the Community Resilience Fund. The following section captures additional testimony provided by the latter three initiatives.

5.5.1.1 Moonshot CVE

Moonshot CVE is a United Kingdom-based initiative. Ms. Ramalingam, Moonshot CVE's co-founder, told the committee that Moonshot CVE has as its goal the development of "online prevention capabilities fit for the 21st Century," explaining that preventative measures must be taken online because that is where extremist recruiting is occurring. She advocated for a pro-active approach, saying:

> We need to ensure that our prevention programming is equipped to pre-empt those crises so we're not just reactive and dealing with violence after the fact, but we're

> pre-emptively going out to individuals who may be at risk in our community and working with them to ensure they know violence isn't the way.

Noting that her organization's research shows members of extremist communities are open to offers of mental health services, Ms. Ramalingam urged government to support the efforts front-line practitioners in mental health support, community outreach and suicide prevention in developing the digital literacy needed to engage extremists online. She highlighted the utility of online advertising tools that "signpost" terrorism prevention counselling services to individuals searching for extremist content. To ensure that such services are locally available to those who need them, Ms. Ramalingam made the following observations and recommendation:

> Here in Canada we need to signpost local services to Canadians engaging with extremist content online. To do this, local providers and networks, like CPN-Prev, need sustained investment to run interventions, extend their service hours, and support professional and mental well-being of staff. These organizations fill a critical gap in Canada's public safety infrastructure. The government should invest in these models and support efforts to take their interventions online, where their services are needed the most.

5.5.1.2 MediaSmarts

MediaSmarts, whose research focuses on Canadian youth interaction with online hate, advocated for a national digital media literacy strategy. Its director of research, Kara Brisson-Boivin, told the committee that,

> Online hate has the power to change how we know what we say we know about scientific and historical facts, social norms and even our shared reality. As youth overwhelmingly turn to the Internet as a source of information, they run the risk of being misled by hate content. If that misinformation is not challenged and users do not have the critical thinking skills to challenge it, some youth may come to hold dangerously distorted views.
>
> Youth need to be supported in developing the skills and knowledge to be able to recognize online hate. This means learning general critical thinking and digital media literacy skills, as well as the techniques and ideologies of hate. In order to talk about controversial topics and have healthy debate, users need to be able to distinguish between arguments based on facts and those that appeal to dehumanization and fear of the other.

Professor Morin reminded the committee of the important role parents have to play in educating their children about IMVE threats such as disinformation, saying,

> I believe that it's essential to make Canadians more aware of these issues so that they can be front-line responders, with the law enforcement agencies backing them up. Allow me to make a comparison. It's as if we entrusted teachers with the entire task of

> educating our children. It doesn't work. The front-line workers in children's education are the parents.

Highlighting the role of social media algorithms in shaping online spaces and promoting hate-filled content, Ms. Brisson-Boivin said a national digital media strategy should not let online platforms "off the hook." Rather, such a strategy would form part of a "whole of society" approach that holds online platforms accountable.

5.5.1.3 Centre for the Prevention of Radicalization Leading to Violence

Montreal-based non-profit, the Centre for the Prevention of Radicalization Leading to Violence, received Community Resilience Fund funding to study the role of families in either contributing to or preventing radicalization to violence. According to its executive director, Louis Audet Gosselin, "the centre promotes prevention through education, outreach and support for individuals in the process of being radicalized and their friends and family."

In discussing the intersection between IMVE narratives and public health measures, Mr. Audet Gosselin said, "the vast majority of anti-health measure activists" had not engaged in violence and that most of the violence his organization had observed entails online threats. He urged a strategy of prevention, "since great anxiety and a heightened sense of insecurity and marginalization are factors."

5.5.1.3.1 Evaluation Required

Thus, throughout Canada, there are various efforts underway to prevent and counter radicalization to violence. However, Mr. Audet Gosselin and Professor Morin highlighted the need to evaluate the effectiveness of these initiatives. Noting that his own centre's collection of testimony from former Neo-Nazis and jihadist militants and sympathizers suggests some degree of success, Mr. Audet Gosselin said that "we would need a broader evaluation program to get a clearer picture of which projects work best." Speaking more generally, Professor Morin said,

> It's essential to have much more rigorous evaluation mechanisms—Canada is headed in that direction—to be able to determine what works and what doesn't, particularly upstream prevention programs. Primary, secondary, and tertiary prevention are all very important today if we are to rectify our practices and adapt how we are all working.

5.5.2 Communities at Risk: Security Infrastructure Program

Witnesses called for improvements to Public Safety Canada's Communities at Risk: Security Infrastructure Program (SIP). Created in 2007 in response to concerns raised by

communities in Canada about their vulnerability to hate-motivated attacks, SIP provides funding for security infrastructure enhancements to at-risk private, not-for-profit organizations such as places of worship, provincially/territorially-recognized private educational institutions, and community centres. Currently, Public Safety Canada covers as much as 50% of the total costs of approved projects up to a maximum contribution of $100,000 per project.[11]

Describing himself as a "big supporter" of SIP, Mr. Koffler Fogel underscored the value of this program to his community, saying "a security guard at Congregation Shaar Hashomayim in Montreal was able to thwart an arson attack on the synagogue because of the surveillance cameras funded in part by the program." He cautioned, however, that cameras alone are not enough to deter the kind of violence being directed at communities of risk. "[Y]ou do need the additional deterrent of power," he said, adding that paying off-duty police officers to be present in front of synagogues and other high-risk communal institutions is no longer financially tenable.

Mr. Farooq shared Mr. Koffler Fogel's views on the importance of SIP but highlighted some of its shortcomings. "[T]he security infrastructure program does not operate effectively as a prophylactic tool," he said, explaining that organizations are required to demonstrate that they are at-risk and this generally requires having experienced a hate-related crime. This, and SIP's "arduous" application process, discourages most mosques in Canada from applying for SIP funding, said Mr. Farooq. Some of these mosques will go on to experience an attack, he said, "at which point, it's far too late." Similarly, Mr. Aziz told the committee that many community organizations that could benefit from this program have neither experience in applying for government funding nor access to resources to that could assist them in this process.

CHAPTER 6: ADDRESSING ROOT CAUSES

Having heard from witnesses such as Professor Bailey about the dangers of an over-reliance on criminal law to address IMVE threats and Ms. Ramalingam about the importance of signposting early, localized and tailored supports to those who are either at risk of being recruited into violent extremist groups or who may wish to leave, the committee came to understand the importance of addressing the root causes of violent extremism. To do so will require a national IMVE framework that will delineate the roles of federal, provincial, territorial and municipal governments as well as civil society organizations, suggested Mr. Fadden.

11 Public Safety Canada, *Communities at Risk: Security Infrastructure Program (SIP)*.

In sharing his experience of serving for 15 years as a Neo-Nazi recruiter and leader in the United States and Canada, Mr. McAleer provided valuable insights about why people join violent extremist causes and under what conditions they will leave.

"Believe it or not, ideology is not the primary drive as to why people join these movements," he said, explaining that "identity, belonging and a sense of meaning and purpose are far greater draws." Adverse childhood events such as trauma, abandonment, or neglect can create psychological vulnerabilities and anti-social behaviours for IMVE recruiters to exploit, said Mr. McAleer, who noted that, by comparison with the 15% of the general population that has suffered childhood trauma, 66% of individuals involved in IMVE movements have experienced "four or more" adverse events.

If the trajectory of vulnerability to IMVE narratives starts early in life, it would stand to reason that efforts to alter this trajectory should start early and use local, non-policing resources that have been trained to address this issue. As Mr. McAleer explained,

> By the time a person gets involved in violent extremism and appears on the radar of law enforcement, several opportunities have already been missed. While there's a growing network of providers, social workers, counsellors and psychologists, for example, for interventions, a more robust effort can be made to engage and train existing resources in the community to utilize their skill set in a way they hadn't considered by creating the opportunities to intervene further upstream, long before law enforcement becomes involved. Training school counsellors would be an example of this.

And because it is not just youth who are being drawn into IMVE movements, Mr. McAleer went on to advocate for community-based programs that address all age groups and are aimed at building resilience against IMVE ideologies.

Helping Canadians who have joined IMVE movements find the "off ramp" is also a matter of pressing importance. Here, witnesses called for compassion and dialogue. They also cautioned against focusing on ideology and hate. Mr. Davies explained that

> The roots of hate often don't start with hate. It starts with a sense of feeling disconnected or a lack of belonging […] Addressing that is as much a function of how we do more positive identity-building work and not assuming necessarily that this is about ideology, per se, or that hate was the beginning foundation.

Mr. Fadden warned that, without dialogue, the various underlying grievances that drove people to participate in the truck convoy will continue to fester. "[I]t would be interesting to know if there's any mechanism today that would allow follow-up to talk to them, other than the police going to see if they can arrest them," he said.

While it would be tempting to use such outreach to “educate,” this would be counter-productive. When engaging radicalized individuals, “never concede,” Mr. McAleer said, and “never condemn.”

CONCLUSION

Each member of this committee is sensitive to the Charter issues that are implicated in responding to the threat of IMVE. Any limitations on freedom of expression must be reasonable and justified in a free and democratic society. The committee believes that there is value in devoting more resources to and engaging more of Canadian society in addressing the human element of IMVE. Greater attention must be paid to protecting those who are the targets of IMVE attacks. As so many witnesses observed, this will require the involvement of every element of Canadian society.

APPENDIX A
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
PayPal Canada	2022/03/03	12
Kevin Pearce, Chief Compliance Officer		
Stripe	2022/03/03	12
Katherine M. Carroll, Global Head of Public Policy		
Gerald Tsai, Head of Compliance		
GiveSendGo	2022/03/03	12
Jacob Wells, Co-Founder		
Heather Wilson, Co-Founder		
As an individual	2022/03/31	16
Aurélie Campana, Full Professor		
Mubin Shaikh, Counter Extremism Specialist		
Centre for the Prevention of Radicalization Leading to Violence	2022/03/31	16
Louis Audet Gosselin, Scientific and Strategic Director		
Insight Threat Intelligence	2022/03/31	16
Jessica Davis, President and Principal Consultant		
The Global Disinformation Index	2022/03/31	16
Daniel J. Rogers, Executive Director		
As an individual	2022/04/26	19
Ilan Kogan, Data Scientist Klackle		
Canadian Anti-Hate Network	2022/04/26	19
Evan Balgord, Executive Director		

Organizations and Individuals	Date	Meeting
Centre on Hate, Bias and Extremism	2022/04/26	19
Barbara Perry, Director Ontario Tech University		
Global Project Against Hate and Extremism	2022/04/26	19
Dr. Heidi Beirich, Co-Founder		
Wendy Via, Co-Founder		
Meta Platforms	2022/04/26	19
Rachel Curran, Public Policy Manager Meta Canada		
David Tessler, Public Policy Manager		
Twitter Inc.	2022/04/26	19
Michele Austin, Director Public Policy (US & Canada)		
As an individual	2022/04/28	20
Dr. Stephanie Carvin, Associate Professor Norman Paterson School of International Affairs, Carleton University		
Dr. Carmen Celestini, Post Doctoral Fellow The Disinformation Project, School of Communication, Simon Fraser University		
Dr. Diana Inkpen, Professor School of Electrical Engineering and Computer Science, University of Ottawa		
Dr. Christian Leuprecht, Professor Royal Military College of Canada, Queen's University		
Brandon Rigato, Lead Research Assistant on Hate and Extremism in Canada Carleton University		
UNESCO Chair in Prevention of Radicalization and Violent Extremism	2022/04/28	20
Dr. David Morin, Co-Chair Université de Sherbrooke		

Organizations and Individuals	Date	Meeting
As an individual	2022/05/05	22
Jane Bailey, Full Professor Faculty of Law, University of Ottawa		
Dr. Garth Davies, Associate Director Institute on Violence, Terrorism, and Security, Simon Fraser University		
Tony McAleer, Author and Co-founder Life After Hate		
Samuel Tanner, Full Professor School of Criminology, Université de Montréal		
B'nai Brith Canada	2022/05/05	22
Michael Mostyn, Chief Executive Officer National Office		
Marvin Rotrand, National Director League for Human Rights		
Center for Countering Digital Hate	2022/05/05	22
Imran Ahmed, Chief Executive		
As an individual	2022/05/10	23
Navaid Aziz, Imam		
Canadian Race Relations Foundation	2022/05/10	23
Mohammed Hashim, Executive Director		
MediaSmarts	2022/05/10	23
Dr. Kara Brisson-Boivin, Director of Research		
Moonshot	2022/05/10	23
Vidhya Ramalingam, Co-Founder		
Tech Against Terrorism	2022/05/10	23
Adam Hadley, Executive Director		
As an individual	2022/05/12	24
Richard B. Fadden		
Vivek Krishnamurthy, Samuelson-Glushko Professor of Law University of Ottawa		

Organizations and Individuals	Date	Meeting
Canadian Security Intelligence Service	2022/05/12	24
Marie-Hélène Chayer, Executive Director Integrated Terrorism Assessment Centre		
Cherie Henderson, Assistant Director Requirements		
Department of Public Safety and Emergency Preparedness	2022/05/12	24
Robert Burley, Senior Director Canada Centre for Community Engagement and Prevention of Violence		
Lesley Soper, Director General National Security Policy		
Royal Canadian Mounted Police	2022/05/12	24
D/Commr Michael Duheme		

APPENDIX B
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the committee related to this report. For more information, please consult the committee's webpage for this study.

B'nai Brith Canada

Carvin, Stephanie

Global Project Against Hate and Extremism

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 12, 16, 19, 20, 22 to 24, 28 to 30) is tabled.

Respectfully submitted,

Hon. Jim Carr, P.C., M.P.
Chair