2022

The Everywhere Threat

RISKS TO CANADIAN SOCIETY IN THE DIGITAL AGE and SOLUTIONS

Foundation for a Path Forward

As an organization founded and based in Vancouver, we are committed to the process of decolonization, and reconciliation with First Nations and Urban Indigenous communities. We acknowledge we are on the unceded territories of the xʷməθkʷəy̓əm (Musqueam), Sḵwx̱wú7mesh (Squamish), and Sel̓íl̓witulh (Tsleil-Waututh) Nations. We thank them for having cared for this land and look forward to working with them in partnership as we continue to build this great home together.

Publication Date: September 2022
Published by: Foundation for a Path Forward

Foundation for a Path Forward is an anti-racist and solutions-focused Resilience building NPO based in British Columbia with branches across Canada.

The Foundation is the First Official Faith Based Community Convener for anti-Racism Initiatives in British Columbia. We offer a multi-faceted, Canada wide approach in identifying and challenging racism by connecting communities with information, support and the training they need to respond to, and prevent future incidents of, racism and hate.

We take an anti-racist and start-up mindset towards developing solutions for key challenges faced by Canadians. Through this lens we are developing and delivering creative and impactful solutions for Racism, Truth and Reconciliation, Climate Justice, Public Safety, Gender Equality, Youth Empowerment, Mental Health, Social Technological Innovations, LBGTQ2S+ Inclusion, Refugee Support, and more.

Since 2020 we impacted 750,000+ people, formed over 200+ organizational relationships and opened offices in Toronto to take the same Silo-Busting, evidence-based approach pioneered in B.C. across the country.

Table of Content

Background:

Canada has two borders: one physical border with the United States that you can see, point to, and walk through, and another digital border with the rest of the globe. This second border is unattended and unprotected.

Every day, Canadians are assaulted over this border. Our digital border enables for the unfettered movement of socially damaging ideas, memes, ransomware, foreign-power propaganda, and hatred, with few mechanisms to prevent, monitor, oppose, or address.

From the infiltration and co-opting of the "Freedom Convoy" movement (whose Facebook page was created in Bangladesh[1]), to the 300+ right wing extremist groups in Canada (many motivated by Transnational White Supremist Ideology), to the ongoing threat of religious-inspired attacks, the rise in antisemitism and Islamophobia, the increasingly violent political rhetoric, and threats against government, to the spread of anti-Asian hatred.

These and other risks may be classified into four categories:

1. Attacks on truth (disinformation and digital manipulation)
2. Attacks on democracy (degrading of democratic norms and institutions)
3. Attacks on society (spread of societal discord and hate)
4. Attacks on infrastructure (cyber-attacks on systems and digital infrastructure – covered in future report)

To combat these threats a whole-of-society effort is needed. Government, non-governmental organisations (NGOs), universities, corporations, religion groups, and the public must be informed of the hazards and challenges of our digital world. This report provides a summary of the identified challenges as well as suggested solutions and calls to action.

Attacks on Truth:

Truth Decay:

According to research conducted by the RAND Corporation[2], over the past two decades, national political and civil discourse in Canada and the United States has been characterised by "Truth Decay," defined as a set of four interrelated trends: an increase in disagreement about facts and analytical interpretations of facts and data; a blurring of the line between opinion and fact; and an increase in the relative volume and influence of opinion and personal experience.

These trends have many causes, but this report focus on changes in the information system, including social media. The degradation of civil discourse, political gridlock, alienation, and

[1] "The Funding Behind 'Freedom Convoy' Protests : NPR." *NPR.org*, 19 Feb. 2022, www.npr.org/2022/02/19/1081987391/the-funding-behind-freedom-convoy-protests.

[2] Kavanagh, Jennifer, and Michael D. Rich. "Declining Trust in Facts and Institutions Imposes Costs on Society." *Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life | RAND*, 16 Jan. 2018, www.rand.org/pubs/research_reports/RR2314.html.

disengagement of people from political and civic institutions, and ambiguity over national policy are some of the most detrimental effects of truth decay.

One item we wish to highlight is that a 2017 study used data on web traffic for the top 609 real-news websites and 65 fake ones (e.g., sites that produce only or mostly articles based on verifiably false information) and compared how individuals accessed those sources, focusing on such methods as direct browsing and social media. The primary access route for real-news websites is direct browsing (followed by search engines), and only 10 percent of traffic gets there via social media. For "fake-news" sites, however, more than 40 percent of traffic comes from social media.[3]

Online Disinformation:

COVID-19 misinformation exemplifies the ease with which social media can be used to spread not simply lies, but potentially life-threatening falsehoods. Researchers discovered that just 12 individuals[4] are responsible for the majority of the false allegations and plain falsehoods regarding COVID-19 vaccinations that circulate on Facebook, Instagram, and Twitter. The 'Disinformation Dozen,' as they've been dubbed, created 65% of anti-vaccine disinformation shares on social media sites.

The Canadian government recognizes the threat and understands that a strong democracy relies on Canadians having access to diverse and reliable sources of news and information so that they can form opinions, hold governments and individuals to account and participate in public debate.

The government states, as part of the Digital Citizen Initiative[5] that "In response to the increase in false, misleading and inflammatory disinformation published online and through social media, the Government of Canada has made it a priority to help equip citizens with the tools and skills needed to critically assess online information."

However, not enough substantive developments have occurred since. There is no reporting system nationwide, nor is there a consolidated and up-to-date database of misinformation and online harms for scholars, policymakers, or community leaders to access. The groups most vulnerable to digital threats are rarely involved – especially in western provinces. Millions of dollars have been spent with few discernible results. An online hate, harm, and disinformation reporting system for national use and resource database is urgently needed in Canada.

---

[3] Hunt Allcott and Matthew Gentzkow, "Social Media and Fake News in the 2016 Election," Journal of Economic Perspectives, Vol. 31, No. 2, Spring 2017b

[4] Bond, Shannon. "Just 12 People Are Behind Most Vaccine Hoaxes on Social Media, Research Shows : NPR." *NPR.org*, 14 May 2021, www.npr.org/2021/05/13/996570855/disinformation-dozen-test-facebooks-twitters-ability-to-curb-vaccine-hoaxes.

[5] Heritage, Canadian. "Online Disinformation - Canada.ca." *Online Disinformation - Canada.ca*, www.canada.ca/en/canadian-heritage/services/online-disinformation.html. Accessed 1 Oct. 2022.

Attacks on Democracy:

According to The Canadian Centre for Cyber Security (CCCS), between 2015 and 2020, the great bulk of cyber threat activities harming democratic processes may be ascribed to state-sponsored cyber threat actors. In pursuit of their strategic goals, these players attack democratic processes (i.e., political, economic, and geopolitical).

Cyber threat actors often attack voters, political parties, and electoral infrastructure. The CCCS believes that cyber threat actors believe that attacking several targets linked with a democratic process is more successful than targeting one group in isolation.

Between 2015 and 2020, cyber threat activities targeted voters more than political parties or elections. This action encompassed both online foreign influence and more classic cyber threat operations, such as information theft or blocking access to vital websites. It is conceivable that cyber threat actors believe that targeting voters is a more effective and relatively simple strategy to disrupt democratic processes.

Online Hate Leading to Political Violence

Canadian politicians are the focus of internet vitriol and incitement to violence. The Minister of Public Safety stated in June 2022 that all members of Parliament will be given mobile duress devices, sometimes known as "panic buttons." This was in reaction to increasing threats and safety concerns for MPs.

A recent report by HillNote[6] examines the scale of political violence in Canada and throughout the globe, with an emphasis on online violence and abuse; the uneven effect of violence on some groups of politicians; and some recent federal and parliamentary measures to combat political violence.

According to the report, online violence against politicians enables attackers to abuse politicians from anywhere, sometimes anonymously, and with little repercussions. Internet violence may be prevalent and long-lasting, given the difficulties of deleting abusive material from online platforms and the possibility for enormous, global audiences.

Abuse aimed towards politicians was frequent on social media platforms throughout previous Canadian federal general elections; for example, in 2019, researchers[7] categorised over 40% of tweets addressed at candidates as uncivil and 16% as abusive. Researchers[8] classified 20% of tweets posted to politicians on election day in 2021 as "insulting, aggressive, or impolite." 37%

---

[6] loprespub. “Violence Against Politicians in Canada and Internationally - HillNotes %.” *HillNotes*, 15 Sept. 2022, hillnotes.ca/2022/09/15/violence-against-politicians-in-canada-and-internationally.
[7] https://democracy2017.sites.olt.ubc.ca/files/2020/10/Trolled_Oct-28.pdf
[8] Admin. “SAMbot Election Day Snapshot: September 20, 2021 | SAMbot.” *SAMbot*, 29 Sept. 2021, sambot.ca/sambot-report-september-20-2021.

of the tweets in this group were categorised as "likely to involve profanities or threatening language." According to the same report:

- Justin Trudeau continued to receive the largest number and proportion of toxic tweets of all candidates tracked, with 21% labelled likely to be toxic.
- Of the 67,436 tweets analyzed:
    - 11,124 were labelled as containing insults
    - 5,451 were labelled as containing profanity
    - 4,892 were labelled as containing identity attacks
    - 4,802 were labelled as containing threats
    - 2,404 were labelled as containing sexually explicit content

Attacks on Society:

Our colleagues at Moonshot (a UK based online digital security company) found that hate and racism spread with the increase in white supremacist narratives and content.

During the research period of July 2020 to March 2021, 511,759 total searches connected to white supremacy were recorded. This initiative was established by Moonshot and the (American Defence League) ADL in reaction to white supremacist activities surrounding real-world events such as the COVID-19 outbreak, large Black Lives Matter (BLM) rallies and counter-protests, and the United States presidential election. These circumstances conspired to make it easier for white supremacists and other violent extremist groups to organise and recruit.

Moonshot and ADL monitored Google searches for 17,279 keywords related to the following search categories: anti-Black; anti-Muslim; antisemitic; the Ku Klux Klan; neo-Nazi / white supremacy; and white supremacist conspiracy theories. The teams conducted ongoing monitoring of extremist media, websites, and influencer accounts to identify and monitor interest in new narratives, slang, memes, events, platforms, and merchandise.

The final paper, "White Supremacy Search Trends in the United States," goes into depth on what this collaboration discovered about how Americans search for violent extremist narratives and material during times of political crisis. The report's key findings include:

- Anti-Black search traffic peaked during the summer of 2020, when systemic racial inequality took center stage in the U.S. during nationwide protests. Violent anti-Black keywords, such as "how to kill black people," sustained high search volumes in July and August of 2020.
- Offline events appeared to catalyze search traffic for extremist content online. Moonshot observed elevated search traffic for anti-Black, antisemitic, and neo-Nazi/white supremacy themes around three major offline events: the nationwide protests against racial injustice throughout the summer of 2020, the presidential election period from 4 September to 6 November 2020, and the period of post-election

uncertainty that led to the storming of the Capitol by domestic extremists on 6 January 2021.

- There was sustained interest in antisemitic websites, white supremacist merchandise and literature, and the Ku Klux Klan, all of which serve as easily identifiable online access points for white supremacist content and group membership.

One of the most difficult issues for the public nowadays is detecting and recognizing when they are being influenced by foreign forces. For example, according to MIT Technology Review[9] in the run-up to the 2020 US election, the most hotly disputed in US history, Eastern European troll farms were running Facebook's most popular pages for Christian and Black American content.

According to an internal corporate assessment, these pages were part of a wider network that together reached roughly half of all Americans, and that reach was gained not via user choice but largely as a function of Facebook's own platform design and engagement-hungry algorithm. As a result, in October 2019, all 15 of the top pages targeting Christian Americans, 10 of the top 15 Facebook pages targeting Black Americans, and four of the top 12 Facebook pages targeting Native Americans were being run by troll farms.

A perfect example of how this can lead to social harm is the case of the Islamic Da'wah Centre of Houston. In 2016, two Russian Facebook pages organized dueling rallies in front of the Islamic Da'wah Center of Houston.[10] Heart of Texas, a Russian-controlled Facebook group that promoted Texas secession, leaned into an image of the state as a land of guns and barbecue and amassed hundreds of thousands of followers. One of their ads on Facebook announced a noon rally on May 21, 2016 to "Stop Islamification of Texas." A separate Russian-sponsored group, United Muslims of America, advertised a "Save Islamic Knowledge" rally for the same place and time.

The problem gets worse when AI is used to accelerate the creation and disbursement of disinformation. Experts from the Center for Security and Emerging Technology (CSET) at Georgetown's Walsh School of Foreign Service teamed the GPT-3 AI system up with humans and tested it across six disinformation activities11. The report cites the Internet Research Agency (IRA), a "troll farm" used to spread Russian propaganda across social media, as an example of a contemporary government disinformation capability.

[9] "Troll Farms Reached 140 Million Americans a Month on Facebook Before 2020 Election | MIT Technology Review." *MIT Technology Review*, 16 Sept. 2021, www.technologyreview.com/2021/09/16/1035851/facebook-troll-farms-report-us-2020-election.

[10] Allbright, Claire. "A Russian Facebook Page Organized a Protest in Texas. A Different Russian Page Launched the Counterprotest. | the Texas Tribune." *The Texas Tribune*, 1 Nov. 2017, www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-russian-page-l.

[11] https://cset.georgetown.edu/wp-content/uploads/CSET-The-AI-Triad-and-What-It-Means-for-National-Security-Strategy.pdf

GPT-3 gives hostile actors an opportunity to scale up disinformation operations as, when it is used with humans, the AI can take on much of the labour. Indeed, when operated by a skilled human, the GPT-3 fooled 88% of readers[12] into thinking text was written by a person.

Solutions: HateShield

A New Approach to Online Safety

HateShield is designed to help us move beyond the discourse around freedom of expression and government censorship to address real challenges in the coordination of information and organizations in dealing with the challenges raised by balancing a free and open society with attacks on national unity and security. We do this by avoiding any direct censorship or take down of content.

The rise in online hate motivated violence, specifically anti-government and anti-democratic is a virus that has infected every corner of the virtual world. Here in Canada, we have seen how its effects translate from online disinformation to real world violence. The HateShield Online Platform seeks to reduce online hate to prevent real-world violence.

HateShield is a comprehensive and multi-sectoral platform. It is an anti-racist and anti-hate online virtual platform for the connection and coordination of government, Asian, Black, Indigenous, and other Peoples of Colour, Faith, 2SLGBTQ+, allied communities and organizations - supported by the development of artificial intelligence systems, for the *detection* (through crowdsourced reporting and AI) and *neutralization* (by providing stakeholders data and information to act) of hate and disinformation online.

The promise of social media was to connect the world and make it a better place. However, it has been compromised by a virus of hate and weaponized. Our mission is to reduce online and offline hate to help prevent real-world violence. Our vision is to connect institutions and individuals on a Virtuous Virtual Network by combining real-world relationships with technology.

The removal of hate content from social media platforms is first and foremost the responsibility of those platforms. However, by understanding where content it is coming from, who is spreading it, and how to effectively neutralize it among members of the public susceptible to it, we can achieve meaningful positive impact now. Canada requires a national database of harmful content and national standards for recognizing and reporting online hate and disinformation.

Canada Wide Standards:

Establishing standards and platform for cross-Canada identifying and recording all instances of disinformation, hate incidents, or verifiably factually inaccurate statements. This requires the

[12] Lowe, Josh. “AI Could Scale up Disinformation Campaigns, Experts Warn.” *AI Could Scale up Disinformation Campaigns, Experts Warn*, www.globalgovernmentforum.com/ai-could-scale-up-disinformation-campaigns-researchers-warn. Accessed 1 Oct. 2022.

coordination of the public, institutions, government, and Artificial Intelligence capabilities. The HateShield Platform will allow for the decentralized crowdsourced as well as AI informed review of data.

Hate Reporting:

HateShield is designed to facilitate the nationwide coordination and communication of organizations and groups operating throughout the country to facilitate the reporting of hate crimes. Urgently required is a simple, user-friendly, and standardized system that can be implemented into the website or app of any organization (through a plug-and-play API). Currently, too many organizations have tools that are redundant, insufficient, or non-functional, few of which automatically exchange information with one another or with Statistics Canada.

Online Hate Predicts Real World Violence

One of the most important reasons for Canadians to better collect and analyze online hate is the direct correlation it has with real world hate crimes. One of the best examples of this comes from the UK.

The Brexit vote in 2016 and 2017 were followed by huge and unprecedented spikes in online hate speech and offline hate crime in the UK. Although the amount of online hate speech grew considerably in the aftermath of all of these incidents, it was less likely to be retweeted and to persist for lengthy periods of time. Where hate speech was retweeted, it came from a small community of individuals who sought out each other's posts. Hate speech, particularly during the Brexit vote, was discovered to be predominantly fueled by a tiny number of Twitter accounts. Only 6% of people contributed almost 50% of anti-Muslim hate speech, many of whom were openly anti-Islam.

Researchers[13] statistically modelled the influence of online hate speech on the incidence rate of hate crimes on the streets to investigate the relationship between online behaviour and offline effects. A surge in racially and religiously aggravated violence, criminal damage, and harassment seems to be linked to an increase in online anti-Muslim and anti-Black rhetoric on Twitter. When adjusting for established predictors of hate crime, such as educational achievement, age, employment, and race, this statistical connection persisted. According to predictions, the occurrence rate of racially and religiously aggravated violence rose by up to 100% in a region with a 70% black and minority ethnic population and 300 hate tweets made every month.

Further examples of the importance of understanding online trends can be seen in the anti-Asian hate comments of former US president Donald Trump. US President Donald Trump's anti-Asian statements "Anti-Asian sentiment depicted in the tweets containing the term 'Chinese Virus' likely perpetuated racist attitudes and parallels the anti-Asian hate crimes that have

[13] "The Connection Between Online Hate Speech and Real-world Hate Crime | OUPblog." *OUPblog*, 12 Oct. 2019, blog.oup.com/2019/10/connection-between-online-hate-speech-real-world-hate-crime.

occurred since" said Dr. Yulin Hswen, the study's principal author and an assistant professor at UC, San Francisco.

The findings, published in the American Journal of Public Health, follow a run of assaults against Asian communities in the United States, including a sequence of shootings in Georgia that killed six people of Asian origin.

The research found a difference in anti-Asian attitude when using neutral hashtags like #COVID-19 vs racist hashtags like #Chinesevirus: 20% of #COVID-19 hashtags had anti-Asian sentiment, compared to 50% of #Chinesevirus hashtags.

Education

In order to support the development of a digitally aware citizenry we have encountered two key challenges: awareness and opportunity. Firstly, there is a lack of awareness among the public regarding the types of risks affecting Canadians. This is more pronounced when looking at the population most affected by disinformation and social media manipulation.

The development of toolkits and infographics to help the average citizen easily identify disinformation or social manipulation is required as part of a holistic approach to online hate and online harms. More in depth toolkits are needed for population-specific (i.e. University student, activist, etc.) participation in HarvestHate Hackathon type events.

HarvestHate

Hosting a yearly national & provincial Hackathon meeting to discuss and build solutions for the rise in hate crimes / disinformation in Canada, coordinate our collective efforts, identify best practices to countering this rise and establish new youth/community led responses.

Artificial Intelligence

Detection of disinformation with community members (crowdsourcing) supported by using AI: AI algorithms will flag suspicious posts and content (for example, from a pool of 100 million tweets in the last 2 years). Community members in the post's location of origin will review a sample set of the AI-flagged posts to provide human feedback about whether the posts were flagged correctly by the AI i.e. erroneous information (factually incorrect) or disinformation (intended to mislead public opinion).

Note: The English word disinformation is a translation of the Russian дезинформация, transliterated as dezinformatsiya, which Soviet planners in the 1950s defined as "dissemination (in the press, on the radio, etc.) of false reports intended to mislead public opinion."

The AI will use the community members' feedback to improve its ability to flag content in real-time and to learn to detect new forms of hate speech and disinformation that arises over time volunteers and update itself to detect new forms of hate speech and disinformation.

The platform is designed to be deployed in multiple formats including as an API plug-in for Canadians and organizations (schools, public funded websites, etc.) to automatically flag and report hate speech, disinformation, verifiably inaccurate or harmful information. Furthermore, users can report and contribute to highlighting new disinformation that is not labeled by the algorithm.

NGO Coordination

The HateShield platform is envisioned to be a way for NGOs across the country to share information, coordinate, and report. Our API plug-in can be integrated into any organization's existing website to empower them with reporting and connecting tools. For a full list of supporting organizations please see Addendum 1.

Real World Hate Reporting

The platform in designed to include (in further updates pending developmental funding) additional features to support not just online harms reporting but also real-world reporting.

The platform's ability for Canadians to flag, capture, and report online and real world hate and harms can be used to empower existing organizational reporting features, create a standardized experience across government, academic, business, and non-profit sectors and allow for the centralization of data collection.

Decision makers and stakeholders will be able to access trends and information in real-time as it is collected across the country. Through discussions with Statistics Canada we learned that such information can even be used to help inform their work and reporting additional information and up-to-date figures.

HateShield is supported by the Province of British Columbia Resilience B.C. Anti-Racism Network, the RCMP, the Vancouver Police Department, the University of British Columbia, the Vancouver Aboriginal Community Policing Centre (VACPC) and more. For a full list of supporters please review addendum 1.

Project Partners and Experts

Masood Hassan – Oracle | Ai Forte Solutions. Masood has managed hundred million-dollar budgets for projects in Canada and the United States. 25+ Years as a Software Engineer who helped architect province wide initiatives in Canada including B.C., Alberta, and Ontario e-health platforms, as well as Obamacare (Affordable Care Act) in the US. Impacting 200 million people by delivering design blueprints & implementation including architecting the security and scalability of Dubai Ports World and Best Buy.

Dr. Ishtiaq Ahmed – University of Toronto. Artificial Intelligence. Assistant Professor of Computer Science at the University of Toronto. Dr. Ahmed directs the Third Space research group at the DGP Lab, a Faculty Fellow at the Schwartz Reisman Institute for Technology and Society, and a Senior Fellow at the Massey College. He co-organizes the monthly UofT Critical Computing Seminar that hosts speakers analyzing computer science and its applications from

the perspectives of marginalization, bias, and oppression. He co-direct the PRISM program at the CS Department that trains students from marginalized communities for higher education in computer science. He also leads the weekly Critical Data Science reading group that studies and analyzes recent scholarly work around AI and Machine Learning from various critical points of view.

Ali Serag – The Defi Ethereum Project. Ali studied Computer Science at UBC, where he co-founded Fostrum, a fintech startup backed by Techstars & Barclays Bank. He chaired Canada's largest tech intern community, organized the country's first diversity and reconciliation parade and worked in various tech companies including SAP where he developed predictive analytics software used at giants like Alphabet Inc. Ali is a member of Global Shapers and harnesses over a decade of software experience towards building the future of Web3. Recently Ali was a collaborator on designing Crypot blockchain platforms with GitCoin, and is a co-founder of LeetCoin.co where he managed the community Di-Fi disbursement of 3 million dollars to community members. Ali enlivens his passion towards Tech for Good, receiving over half-a-dozen tech awards and creating several not-for-profit initiatives. His most recent open-source project, CovidImpact, unlocked $3B in small business aid during the pandemic and was supported by IBM, SAP & UNESCO.

(Name asked to be withheld from public testimony) Head of Amazon Simple Queue Service (SQS) at Amazon Web Services (AWS) | Codify Academy Co-Founder: Over a decade of experience in teaching technology to youth and in developing large scale enterprise applications which generated over a hundred-million-dollar yearly revenues. Held senior roles throughout the product life cycle in multi-site, cross-continent projects. Co-founder of Codify Academy a technology education platform for marginalized Canadian children.

Tariq Tyab Foundation for a Path Forward Tariq Tyab has 25 years experience in community service. He has built interfaith bridges and helped empower IBPOC communities. Tariq is co-founder of the Faith Based Community Convener for Anti-Racism Initiatives in the Province of British Columbia, Foundation for a Path Forward. He is also co-founder of the Muslim Food Bank and Community Services, the Muslim Care Centre and Islam Unravelled. Tariq is a former executive with the BC Muslim Association. Tariq is also CEO and Co-founder of a social enterprise company, Ai Forte Solutions, which is developing anti-Hate technology (HateShield) and refugee support platforms (RefugeeShield)

Yusuf Siraj Foundation for a Path Forward Co-Founder Foundation for a Path Forward | Ai Forte Solutions. 10+ years' experience in marketing, digital advertising, content creation, and promotion for businesses and NGOs. Subject matter expert on digital harms, Islamophobia, and digital democracy.

Funding Needs

Government support is required to go ahead and establish a consolidated standard for Canada (and the possibility to export Canadian technology/solutions to other democracies and allies across the globe). Combating the dangers of online disinformation and harms demands partners to understand and address them in real time.

Funding is required for retaining talent, growing the platform to meet national security requirements, investing in educational and awareness initiatives, and enhancing database capacity and security.

To protect our physical boundaries and airspace, Canada plans to spend $19,000,000,000 on 88 jet fighters from the United States. We can develop a platform to help secure our digital boundaries and cyberspace for $4 million. We are requesting that the government take the issue of online harms seriously and invest in Canadian solutions that can not only be used at home, but also exported abroad.

Security and Privacy

We based our project on the highest standards of security and privacy. This includes hosting data in Canada or countries with equivalent or greater personal data security laws. We follow the user-centric design standards of Humane Technology Development, resulting in informed use of data and user consent. This means that at multiple touch points anyone sharing their personal data is informed, clearly, how, by whom, when, and why their data will be used and the option to opt out of data collection is given.

Foundation for a Path Forward

The Everywhere Threat:
Solutions for Digital Harms (HateShield)
Addendum 1

List of Supporting Organizations:

- The RCMP
- Vancouver Police Department
- Metro Vancouver Transit Police
- Vancouver Aboriginal Community Policing Centre
- Canadian Anti-Hate Network
- Chinese Canadian National Council for Social Justice
- Statistics Canada
- The University of British Columbia
- The University of Toronto
- Toronto Metropolitan University (Formerly Ryerson)
- University of Manitoba
- Canadian Municipal Network on Crime Prevention
- The Province of B.C. Anti-Racism Secretary
- Resilience B.C. Anti-Racism Network with 46 spokes in different cities across the province
- The African Arts and Culture Centre (Official Black Community Convener for B.C.)
- BC Association of Aboriginal Friendship Centres with 25 locations across B.C.
- Vancouver Aboriginal Community Policing Centre
- Lifeline Afghanistan
- Chinese Canadian National Council for Social Justice
- ISSofBC
- BC Refugee Hub
- Muslim Food Bank and Community Services (MFBCS)
- Future Ready Initiative
- S.U.C.C.E.S.S.
- Khalsa Aid
- MOSAIC
- Human Concern International (HCI)
- International Development and Relief Foundation (IDRF)
- Jewish Federation
- World Sikh Organization (WSO)
- BC Muslim Association (BCMA)
- Jewish Immigrant Aid Services (JIAS)
- The United Church of Canada
- Islam Unravelled