Understanding and Countering Gendered Disinformation

A framework for resilience and action

May 2025

Executive Summary

CSKA Community Safety Knowledge Alliance

SAPPER LABS

This page is intentionally left blank

This work was prepared by:

www.cskacanada.ca www.sapperlabs.com

With funding from:

Canada

Authors of report

Janos Botschner, PhD
Giovanna Cioffi, CD, PhD
Dave McMahon, MSM, BEng
Julie Ollinger, PhD
Bradley Sylvestre, MA
Ritesh Kotak, JD
Cal Corley, MBA

Additional contributors

Additional support to this project was provided by Actua (www.actua.ca). The following individuals co-authored knowledge products for parents, youth and educators in collaboration with the project team. These resources were produced by Actua in partnership with CSKA:

Janelle Fournier, PhD (ABD)
Mikayla Ellis, BA
Abbey Ramdeo, MT

Suggested report citation:

Botschner, J., Cioffi, G., McMahon, D., Ollinger, J., Sylvestre, B., Kotak, R. & Corley, C. (2025). Understanding and countering gendered disinformation: A framework for resilience and action. Ottawa ON: Community Safety Knowledge Alliance.

Correspondence:

Jbotschner[at]cskacanada[dot]ca

About the Community Safety Knowledge Alliance

The Community Safety Knowledge Alliance is a non-profit applied research organization that supports governments, police, public health and human service leaders in developing, implementing and assessing new approaches to enhancing community safety and well-being service delivery and outcomes.

Over the past decade, CSKA has conducted interdisciplinary research on some of Canada's most pressing social issues, including intimate partner violence, youth radicalization to violence, cybersecurity, food security, drug policy, human rights-based policing, and community reintegration initiatives. CSKA maintains an active posture on issues such as disinformation and artificial intelligence to support adaptive responses to these emerging challenges.

About Sapper Labs Group

Sapper Labs Group conducts research to understand the methods and impacts of disinformation and influence campaigns and networks and as input to the development of processes to support effective countermeasures. SLG is supported by global partners and a comprehensive intelligence sharing network.

The goal of SLG is make the world a better safer place in line with objectives around: countering foreign interference and influence, countering radicalization and extremism, supporting human rights and other activities involving capacity building related to information integrity.

ACKNOWLEDGEMENTS

The authors would like to express sincere appreciation to the following individuals/groups for the guidance they provided to this work. The contents, conclusions and recommendations are those of the authors, alone.

Project Advisory Committee

Michael Doucet, former Executive Director, National Security Intelligence Review Agency
Jennifer Flanagan, Chief Executive Officer, Actua
Carmen Gill, Professor, Department of Sociology, University of New Brunswick
Jennifer Irish, Director, Information Integrity Lab, University of Ottawa
Alan Jones, Executive Advisor, Professional Development Institute, University of Ottawa; former Assistant Director, Canadian Security Intelligence Service
Marcus Kolga, Founder and Director, DisinfoWatch; Fellow, MacDonald-Laurier and Conference of Defence Associations Institutes

Development of Knowledge Products

For parents and educators

Actual National STEM Educator Community of Practice
Actua staff and Actua Network members

For youth

Actua National Black Youth in STEM Program Youth Delegation
Actua Indigenous Youth in STEM Program Youth Delegation
Actua staff and Actua Network members

For police and community groups

Delta Police Department

André Cruz
Communications Assoc.

Cst. Derek Defrane
Domestic Violence Unit

Kim Gramlich
Mgr., Victim Services

Sgt. Alex Quezada
Vulnerable Sector Unit

Greater Sudbury Police Service

Det. Sgt. Adam Demers
Criminal Investigations/ Intimate Partner Violence

Dan Gelinas
Community Mobilization Liaison

Det. Sgt. Lee Rinaldi
Major Sex Crimes

Sudbury YWCA

Marlene Gorman
Executive Director

EXECUTIVE SUMMARY

Today's interconnected world provides a wealth of opportunities for those wishing to harm women, girls and gender diverse persons individually and at scale. This report describes the mechanisms, impacts, and actors behind technology-enabled gendered disinformation. This is not just a gender issue – it is also a socioeconomic and public safety issue which, in some cases, may also become a national security concern. We illustrate why action is needed now and chart a theory- and evidence-informed path forward.

Technology-enabled gender-based violence – including disinformation – draws from a powerful arsenal of tools. It can be used for illicit surveillance (such as monitoring movement and communications) and to manipulate aspects of the built environment (such as features of "smart" homes and vehicles). It can also be used to pollute the information space with deceptive narratives. Gendered disinformation poses a dual threat: it endangers individuals, especially women and gender-diverse people who are often its direct targets; and it undermines society by eroding trust and cohesion, silencing voices, and weakening democratic norms and processes.

Members of certain populations – notably, marginalized and racialized women, girls and gender diverse persons – may disproportionately encounter greater levels of gendered disinformation. Indigenous women and girls in Canada often face gendered disinformation and related violence due to historical biases, colonial legacies and contemporary social media narratives that can often perpetuate harm.

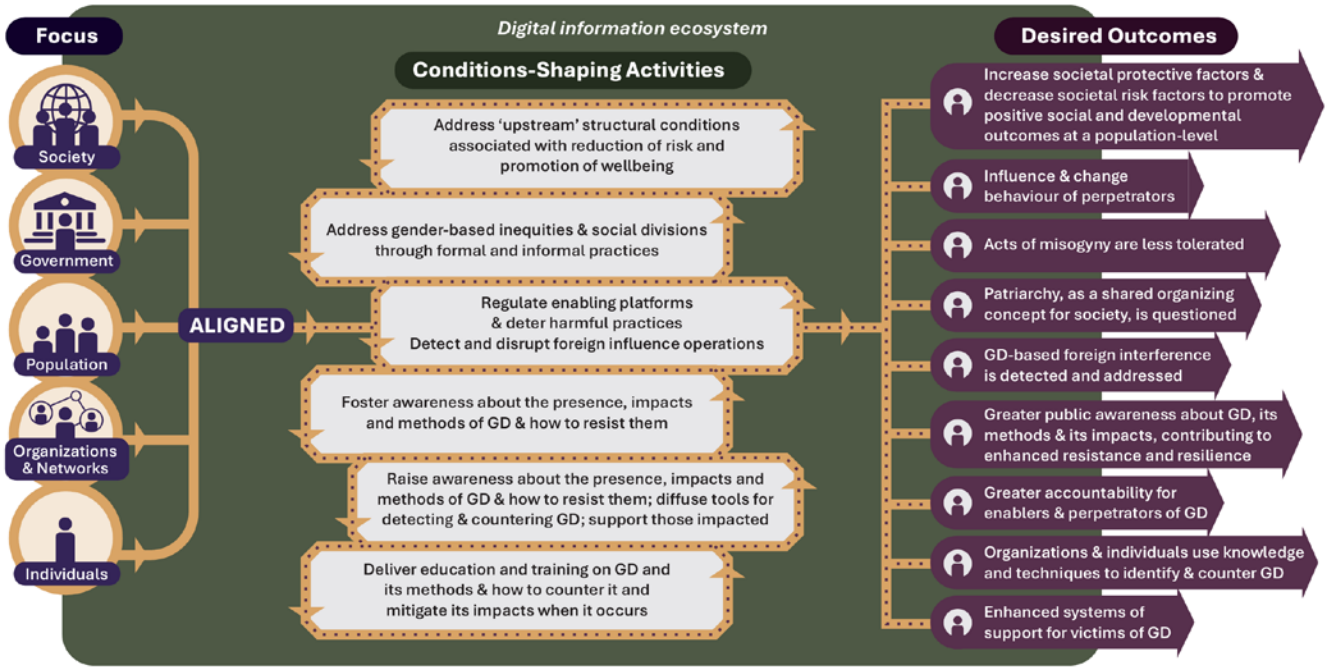
Gendered disinformation is not spread by chance. It can be driven by individual actors, aligned domestic and transnational ideological groups, and even nation states that seek to destabilize democratic societies. When foreign governments are involved, GD becomes an instrument used to sow division, fear, and mistrust across borders – sometimes as a component of broader influence or cyber operations. At a time when online spaces too often amplify misogynist voices and targeted abuse, understanding and countering gendered disinformation has never been more urgent. It is a shared threat across society. Consequently, the resolve and the ability to address gendered disinformation must be a matter of shared responsibility.

The widespread occurrence of gendered disinformation around the world, often leading to violence, underscores the need for international cooperation. This is essential to address the complex, cross-border nature of the issue effectively. By sharing best practices, resources, and intelligence, countries can develop unified strategies to combat disinformation. Domestically, integrating these global insights into national policies and practices will enhance local efforts, ensuring that responses are comprehensive and culturally relevant. Joint initiatives can also strengthen diplomatic relations, promote gender equality, and uphold human rights on a broader scale.

This report provides a novel perspective on gendered disinformation, including a framework for action with a corresponding system of people, processes and technology. Furthermore, it provides a short set of pragmatic recommendations that will have significant impact on combatting gendered disinformation, enhancing human rights protection, and promoting gender equality. These elements are accompanied by a set of information resources for key stakeholder groups seeking to raise awareness and to counter this complex, multi-layered problem.

Building the capacity to counter gendered disinformation will require collaboration. As we navigate geo-political and domestic tensions that threaten the cohesion, unity and sovereignty of Canadian society, our willingness to confront and respond to gendered disinformation will shape the resilience and inclusivity of our digital, democratic and social spaces for years to come.

A preliminary theory of change for addressing gendered disinformation is depicted below. This is discussed in further detail at Figure 9 in this report.



This theory involves multi-level efforts designed to align and create mutually reinforcing conditions, significantly enhancing the likelihood of achieving a range of desired outcomes.

Conclusions

Addressing gendered disinformation is crucial for safeguarding human rights, promoting gender equality, and upholding democratic values. This issue, intertwined with polarization, patriarchy, and misogyny, targets women, girls, and gender-nonconforming individuals, causing harm. A strategic, multi-layered approach is necessary to combat this, focusing on awareness and a coordinated

response. Strengthening resistance to such disinformation requires collaborative efforts to prevent risks, enhance resilience, and align solutions with democratic principles.

Gendered disinformation about Indigenous women and girls in Canada is exacerbated by a colonial history that persists today, reinforcing harmful stereotypes and ignoring ongoing violence. Multi-faceted efforts must be undertaken to break this cycle by challenging false narratives, reforming media practices, and prioritizing Indigenous voices in storytelling. Such measures are vital for transforming the information landscape and supporting reconciliation.

The path forward emphasizes multi-sector collaboration and building broad-based networked capacity to counter gendered disinformation. Increasing awareness and developing new knowledge will be central to this effort. This approach should foster mutual benefits and support collective learning, planning, implementation and further research.

We propose a comprehensive theory of change involving strategically aligned, society-wide interventions grounded in the leading research. This approach includes providing a robust set of knowledge resources and technology examples beneficial to professionals in human services, policy-making, and national security. Furthermore, we recommend creating a cross-sectoral network dedicated to knowledge development and mobilization. This network will support evidence-based, collaborative efforts, ensuring that interventions are informed by the best available evidence and practices. By fostering cooperation across multiple sectors, this critical issue can be tackled effectively and holistically.

Recommendations:

Policy, Legislation and Enforcement

1. That the federal government:

    a. Implement policy and legislative measures to counter gendered disinformation, recognizing that it is a threat that spans community safety and wellbeing, and national security.
        - *The corresponding regulatory framework should ensure platform accountability, transparency, and meaningful financial penalties for non-compliance.*

    b. With targeted investment, initiate cross-departmental, industry, academic and private sector operational coordination and program collaboration to address gendered disinformation within public safety, public health, digital regulation, defence and national security frameworks.

c. Develop a national strategy on gendered disinformation in close partnership with the private sector, research and civil society, integrating public safety, digital governance, and foreign policy approaches.

d. Convene and engage women's advocacy organizations, racial justice groups, security and intelligence professionals, academic researchers, cyber-security experts and relevant community and private sector entities in dialogue on such matters as how to optimize the balance of protection and enforcement with freedom of expression online.

e. Increase data collection and monitoring of gendered disinformation trends and actionable current intelligence.

f. Conduct periodic cross-sector consultations with experts in gender-based violence, cybersecurity, open source intelligence, national security, and digital regulation to understand the evolving landscape of gendered disinformation.

g. Establish gender-responsive online safety laws that hold technology platforms accountable. Options include the re-introduction of Bill C-36 and the applications of relevant elements of a Clean Pipes Strategy.

h. Enhance training for security, intelligence, diplomatic, defence, law-enforcement and policymakers on technology-enabled GD.

i. Invest in digital literacy, research, open source intelligence and enforcement mechanisms to strengthen Canada's resilience against gendered disinformation.

Research and Knowledge Mobilization

2. That the Government of Canada support the creation of a cross-sectoral knowledge mobilization network on gendered disinformation – the Gendered Disinformation Knowledge Network (GenD-Net).

   Such a network would serve as a hub for leadership, information sharing, education and training, research, and policy coordination, program planning, operational coordination and de-confliction ensuring that responses to gendered disinformation are evidence-based, and aligned across sectors.

   The objectives of the network will be to:

   - *Enhance knowledge mobilization and public awareness of gendered disinformation.*
   - *Support curriculum development, stimulate and contribute to education and training.*

- *Strengthen community and cross-sectoral dialogue and collaboration on policy development.*
- *Support defence, intelligence, police and public safety agencies.*
- *Advance research and innovation, including evaluation capacity building.*
- *Bridge gaps in service provision for affected communities.*

Gendered Disinformation as a National Security Issue

3. That the Government of Canada refine and implement options for countering gendered disinformation as a national security issue, including its use as an element of foreign interference. Enhance the capabilities of defensive cyber operations in relation to this threat. More particularly:
    a. Establish a dedicated government funding stream for research and innovation on gendered disinformation that is open to Canadian industry, academia and not-for profit organizations.
    b. Incentivize Canadian industry participation and innovation through public-private partnerships and direct investment.
    c. Develop a national strategy on gendered disinformation as a foreign interference threat, and ensure integration with national defence policy, cyber security and national security strategies.
    d. Fund the creation of a cross-sectoral intelligence-sharing network to combat gendered disinformation, including the creation and maintenance of a national gendered disinformation threat landscape reporting capacity; this would, in-turn, feed into an intelligence "dashboard" (Figure 11) which could be made publicly available as part of building overall awareness an public will to confront this problem (See Annex E4, Attachment B).
    e. Establish legal and policy frameworks to protect women in public life from both foreign and domestic online harm.
    f. Develop a rapid response mechanism to protect individuals facing high-risk disinformation attacks (see Annex E4, Briefing Resources 1 and 4).

Impact of Recommendations

Implementing these recommendations will have significant impacts on combatting gendered disinformation, enhancing human rights protection, and promoting gender equality. By addressing this issue, intertwined with polarization and misogyny, we can safeguard women, girls, and gender-nonconforming individuals from targeted harm. More specific areas impacted are as follows:

Policy and Legislation

By implementing comprehensive policies and legislation, the federal government will strengthen community safety and national security. Establishing regulatory frameworks with platform accountability and penalties for non-compliance will ensure that digital spaces are safer and more transparent. Cross-departmental coordination will enhance efforts to address gendered disinformation within public safety and national security frameworks.

Multi-Sector Collaboration

Creating a national strategy in partnership with the private sector, research institutions and civil society will integrate approaches to enhancing both public safety and social media governance. Engaging diverse organizations in dialogue will balance safety and security with freedom of expression. Furthermore, this approach will help build resilience against gendered disinformation through enhanced data collection, training, and digital literacy investments.

Research and Knowledge Mobilization

A dedicated funding stream for research and innovation, alongside public-private partnerships, will drive industry participation and technological advancements.

Establishing the Gendered Disinformation Knowledge Network (GenD-Net) will enhance public awareness, support curriculum development, and foster cross-sectoral collaboration. By bridging gaps in service provision, it will ensure evidence-based responses aligned across sectors.

National Security

Recognizing gendered disinformation as a national security issue will help refine strategies to counter foreign interference. Developing a rapid response mechanism and legal frameworks will protect individuals from high-risk disinformation attacks.

Overall, when implemented, these measures will help to transform the online information landscape, support reconciliation, and uphold Canadian liberal democratic values by fostering a coordinated, strategic response to gendered disinformation.

Annex A: Project Team

Community Safety Knowledge Alliance

Dr. Janos Botschner, PhD – *Project Lead.* Janos is a social scientist with deep experience in applied research and evaluation and strategic consulting across a range of contexts. He holds a joint doctorate in applied social and developmental psychology. Janos has held a number of adjunct faculty appointments and administrative positions during a lengthy career in the broader public sector. Janos' professional work covers the spectrum of issues related to collaborative public safety and community well-being, with a focus on understanding, and responding adaptively to, the complex issues and emerging opportunities of today's world.

Cal Corley, MBA Cal is CEO of the Community Safety Knowledge Alliance and a former Assistant Commissioner of the RCMP. Over the course of his career, Cal gained extensive experience in both operations and executive management, serving in such areas as national security, criminal intelligence, drug enforcement, human resources, and leading reform initiatives. He also served on secondments at the Privy Council Office and at Public Safety Canada.

Ritesh Kotak, JD, MBA is a Technology and Cybersecurity analyst and a licensed lawyer in Ontario. Ritesh started his career in public safety working for two police organizations focusing on cybercrime investigations and innovation. He left policing to pursue an MBA and then worked in Big Tech for two years focusing on innovation and smart cities. He left the Tech sector to attend law school and received a JD with a Law and Technology Option. Ritesh is a frequent contributor on mainstream media and is an international public speaker. Ritesh has also appeared twice as a witness in House of Commons Committees.

Sapper Labs Group

Dave McMahon, Hon. B.Eng., M.S.M. – *Project Co-Lead.* Chief Intelligence Officer at SLG, Dave is a deep generalist and expert with 40 years of experience in intelligence operations, cyber and cognitive warfare. He has an honours degree in Computer Engineering from the Royal Military College of Canada. Dave served with the Canadian Armed Forces, the Canadian Security Intelligence Service (CSIS), the Communications Security Establishment (CSE), the Security Intelligence Review Committee (SIRC), and the Office of the Communications Security Establishment Commissioner (OCSEC). He was a principal architect of a number of national offensive cyber and foreign intelligence programs for Canada. Dave co-chaired the interdepartmental committee on Information Warfare and psychological operations.

Dr. Giovanna Cioffi, CD, Hon. BA, MDEM, MES, PhD, served as an Army intelligence analyst r and expert in Cyber warfare and Psychological Operations. She was Deputy Chief of Targets/Ground Force Analyst/Special Purpose Reconnaissance Analyst (Operation IMPACT), a Captured Equipment and Material Analyst (Digital Forensics) (Op IMPACT), and a National Security Team Open Source Intelligence Analyst with a multinational joint intelligence task force covering global extremism.. She also worked as an Intelligence Operator and Intelligence Analyst at CANSOFCOM as well as Civil Military Cooperation and Psychological Operations Analyst/Tactical Operator with the CAF.

Dr. Juliane Ollinger, PhD is a research scientist with a PhD in Microbiology (Cornell 2008) with a focus on infectious diseases. Julie brings her strong research background and critical analysis skills to the Sapper team and has contributed to intelligence investigations focused on Due diligence, National Security, Foreign Interference, Disinformation and Support to Defence Operations.

Bradley Sylvestre, MA is an analyst with Sapper Labs Group focused on open-source intelligence (OSINT) and strategic analysis. His research interests broadly encompass strategic competition, foreign interference, espionage, disinformation and deep fake research. Prior to joining Sapper Labs Group, Bradley worked as a strategic analyst with the Canadian Armed Forces and Department of National Defence. Within the force development enterprise, his efforts supported work to identify the necessary capabilities to enable and sustain the Canadian Armed Forces and missions through current intelligence. Bradley holds a MA in International Affairs from the Norman Paterson School of International Affairs (NPSIA), also located in Ottawa.

Actua

Actua and CSKA collaborated to produce resources tailored to parents, youth and educators, based on knowledge synthesized by CSKA and SLG. The following staff members led Actua's involvement in this work.

Mikayla Ellis, BA, Senior Manager, Outreach.

Janelle Fournier, PhD (ABD), Senior Manager, Education.

Abbey Ramdeo, MT, Manager, National Educator Learning Program.

Annex B: Advisory Committee

Michael (Mike) Doucet is a senior leader of portfolios focusing on public safety and technology. He served as executive director of the Security Intelligence Review Committee, now known as National Security and Intelligence Review Agency. He currently serves as Executive Director, Office of the CISO, at OPTIV, a cyber advisory and solutions company, providing strategic advice on cyber programs, technology and risk.

Jennifer Flanagan is the President and CEO of Actua, which has become Canada's largest STEM outreach organization. It represents a national network of 43 universities and colleges that engage youth, ages 6-26, in STEM learning experiences, and advancing equity, diversity and inclusion in STEM. Actua's activities annually reach 350,000 young people. In 2021, Jennifer was awarded in the Manulife Science and Technology category, which recognizes women in STEM roles who are challenging the status quo for knowledge and female empowerment.

Dr. Carmen Gill is a professor in the Department of Sociology at the University of New Brunswick. She works in partnership with police agencies in Canada. Her research focuses on police intervention in intimate partner violence (IPC), domestic homicide and treatment of perpetrators and victims through the criminal justice system. Carmen is currently leading a three-year national research project entitled: Coercive control, risk assessment and evidence of intimate partner violence: Police response in partnership with the Canadian Association of Chiefs of Police (CACP), the Canadian Police Knowledge Network (CPKN) and l'École nationale de police du Québec. Carmen was previously the leader of the Canadian observatory on the justice system response to intimate partner violence (2006-2016). She led the development of the national framework for collaborative police action on IPV with CACP.

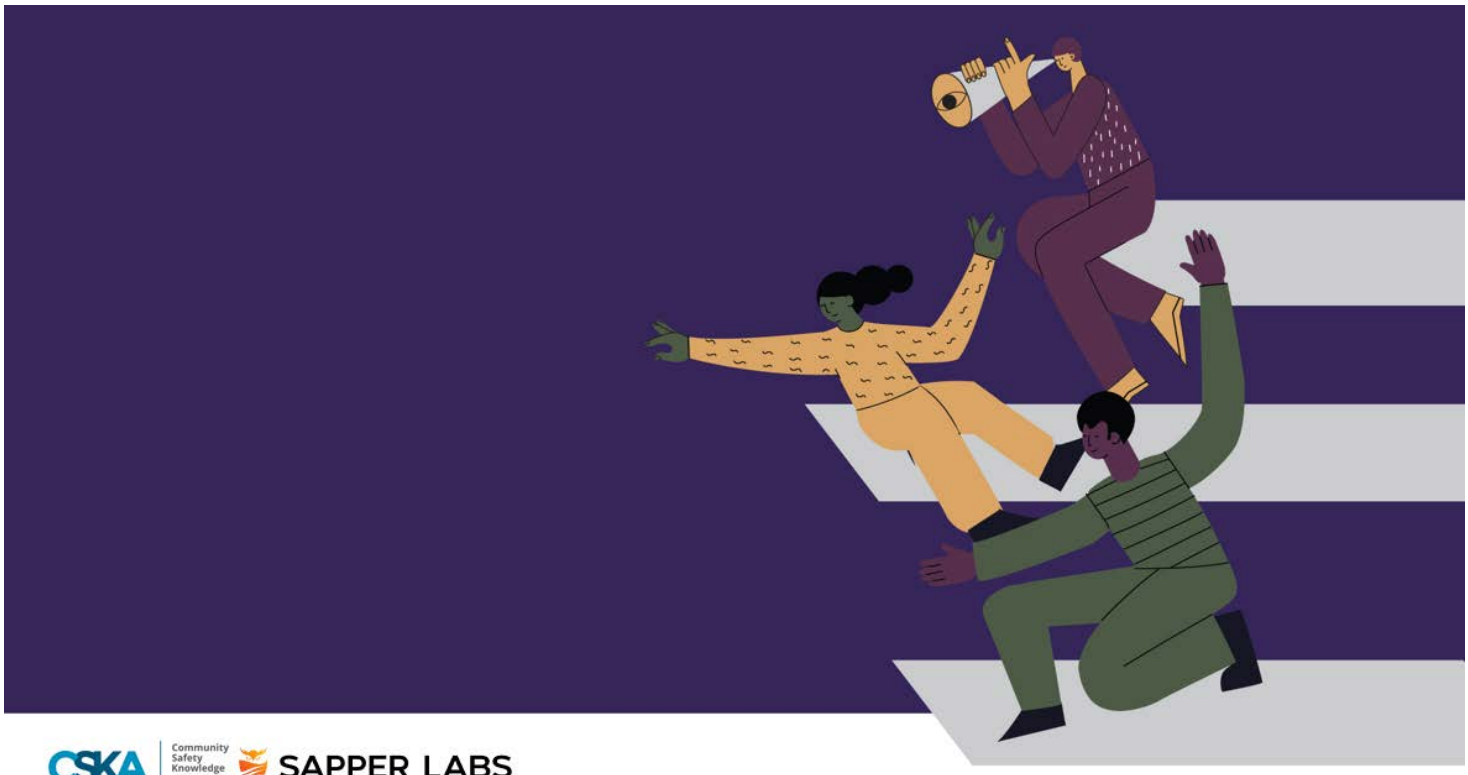
Jennifer Irish has more than 20 years of experience in foreign service and diplomacy. She has been appointed to postings in various embassies across the world, and has been a part of Canada's Permanent Missions to the United Nations in Geneva and New York. In addition to serving three terms in Canada's Privy Council Office, she worked as Director General at Canada's Integrated Terrorism Assessment Centre. Jennifer currently works as an Associate at University of Ottawa's Telfer Centre for Executive Leadership, co-directing its Canada Security and Intelligence Leadership program and teaching accountability, critical thinking, and strategic communication to Canada's next generation of leaders.

Alan Jones is executive adviser to the University of Ottawa Professional Development Institute and a retired CSIS officer who served in numerous operational and policy positions, including assistant director of CSIS. Alan's CSIS career included being the Chair of the G8 working Committee on Terrorism, Senior Policy Advisor in the Privy Council Office, Security and Intelligence Secretariat, Director General of the Counter Terrorism Branch and Director General of the International Terrorism Branch. In 2008 Alan became the Assistant Director for Operations, responsible for all

operational programs and in 2010 he became the Assistant Director for Technology which included both corporate and operational technology.

Marcus Kolga is an international award-winning documentary filmmaker, journalist, digital communications strategist, and a leading Canadian expert on Russian and Central and Eastern European issues. Marcus has a focus on communications and media strategies as tools of foreign policy and defence, and continues to write commentary for national and international media including the Globe and Mail and Toronto Star. He is the co-founder and publisher of UpNorth.eu, an online magazine that features analysis and political and cultural news from the Nordic and Baltic region. Marcus is involved with international human rights organizations and national political organizations. In 2015, Marcus was awarded the Estonian Order of the White Star by President Toomas Hendrik Ilves.

This page is intentionally left blank



CSKA Community Safety Knowledge Alliance

SAPPER LABS