Western University

Scholarship@Western

2022

Cyberpolicing in Canada: A Scoping Review

Laura Huey
Western University, lhuey@uwo.ca

Lorna Ferguson
Western University, lfergu5@uwo.ca

Cyberpolicing in Canada: A Scoping Review

Abstract:

A recent stream of government efforts have surfaced in an attempt to tackle cybercrime in Canada and improve law enforcement responses to cybercrime, such as funding, actionable intelligence, and the creation of new policing response units. However, we know little of 'what works' with respect to cyberpolicing, meaning that these endeavours, and policymakers and funding organizations, are operating without such insights. Therefore, this study sought to conduct an evidence assessment into research on cybercrime-related topics through a scoping review. Our findings show that the overall volume of Canadian cyberpolicing literature is low, and many important subjects are entirely lacking in research. Additionally, we found a distinct shortage of independent or rigorous evaluation of cyberpolicing strategies. From these findings, we offer a range of critical recommendations to improve the state of Canadian research on cyberpolicing.

Cyberpolicing in Canada: A Scoping Review

Introduction

In March 2020, the Royal Canadian Mounted Police (RCMP) announced the testing of a new cybercrime reporting program developed through a joint initiative with the Canadian Anti-Fraud Centre. Anticipated to launch to the public in 2023, the goal of the new online reporting system is to increase police knowledge, tracking and investigation of online crimes through an enhanced reporting system (see RCMP 2021). This initiative is only one piece of a larger public investment by the Canadian federal government at responding to cybercrime that includes sizeable funding for strengthening collaborations between national and international law enforcement, producing actionable intelligence on cybercrime, and creating new policing response units.

While such investments are much needed, what have not kept apace are research and evaluation of existing cyberpolicing efforts and strategies. Nor, until relatively recently, have we seen significant public investments aimed at developing and testing innovative, evidence-based approaches. Thus, borrowing from the language of evidence-based policing, when it comes to cyberpolicing, we know very little about 'what works' (Sherman 1998; Sherman et al. 2002). This is particularly the case in the Canadian context, as detailed in this paper.

To develop a program of Canadian-based cyber-research that will inform sound public policy and practice entails a deeper understanding of the strengths and limitations of the current research evidence base. To that end, we have conducted what will be the first in a series of evidence assessments on research into cybercrime-related topics. Therefore, in this paper, we present a scoping review of the Canadian research literature on cyberpolicing, intending to answer three important research questions:

> RQ1: What is the nature and scope of Canadian cyberpolicing research as
> represented within peer-reviewed journals over the past 20 years (2001-2021)?

RQ2: What is the nature and scope of Canadian cyberpolicing research as represented within the 'grey literature' over the past 20 years (2001-2021)?

RQ3: What Canadian cyberpolicing topics are missing from the literature?

Method of Inquiry

To address the above research questions, we conducted a scoping review (SR). A SR is an exploratory form of knowledge synthesis that allows researchers to understand better what work has been undertaken in a given field (Arksey and O'Malley 2005). SRs are similar to other review methodologies, such as systematic reviews, in that they require a replicable, systematic, and structured search for and the inclusion of literature materials. Though, they differ by allowing the search criteria to be changed post-hoc as one becomes more familiar with the literature, and they do not involve an assessment of the literature quality (ibid.). Given that it was expected that there would be a limited number of studies, and to have the ability to include grey literature, this method was thought more suitable for the purposes of this study. In the pages that follow, we explore the types of topics previous researchers have undertaken, the data sources and methodologies employed, as well as the years and scholarly fields in which studies were produced. Using this technique will help to provide an assessment of not only what is currently available to inform public policy and practice but also, and perhaps more importantly, where we should be focusing future research efforts.

Search Strategy

To construct our search strategy, we had to make several decisions as to what types of material we would be searching for and where we would be looking. We expected that the overall volume of Canadian studies published in peer-reviewed journals in this area would be low, thus early on, the decision was made to include both peer-reviewed published research and studies

found within the 'grey literature' – that is, government and non-governmental reports, Masters theses and doctoral dissertations. We also anticipated that, given the estimated low volume of available material, we would have to search as widely as possible. To that end, we decided to begin by searching academic databases using a university search engine with access to PsycINFO, Criminal Justice Abstracts, PubMed, Web of Science, Scholars Portal, and Sociological Abstracts, among others. Once we had exhausted our ability to find useful material through this method, we turned to the Google search engine to look for government and NGO reports before focusing our efforts on Google Scholar.
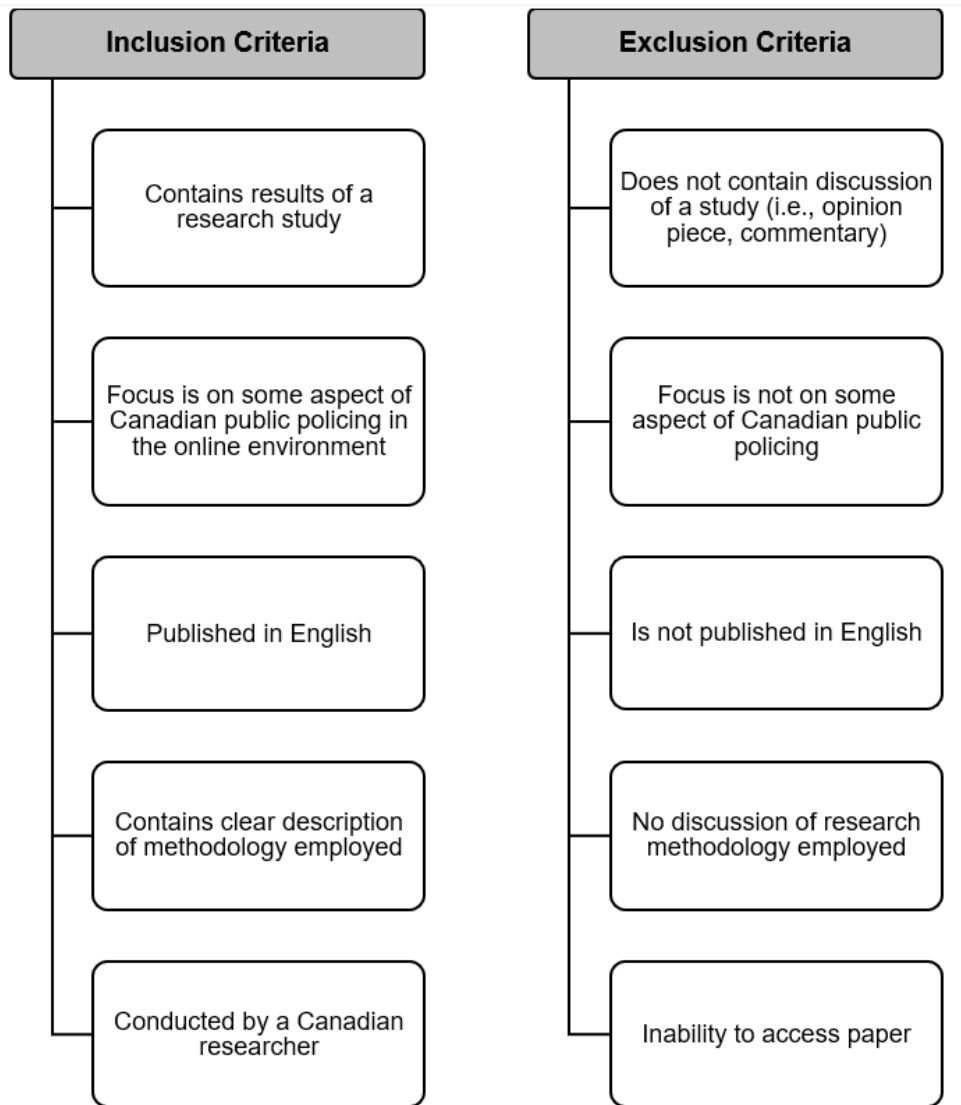
All searches were conducted using keywords, and the date range was set to 2001 to 2021. Keywords used included iterations and combinations of 'Canada,' 'Canadian,' 'police,' 'policing,' 'cyber,' 'Internet,' 'online,' 'research,' and 'study.' We typically stopped reading search results at the 100th result, as at that point, most results were no longer relevant. To arrive at our final sample, the abstracts of returned results were first read in full, and an initial decision was made as to whether to include or exclude as a result. If it was not clear after reading the abstract whether a paper met the inclusion criteria as noted below, it was downloaded and read to assess its applicability to our topic. After each of the downloaded articles was reviewed against the inclusion criteria, we arrived at a final sample of a collection of 18 studies.

Inclusion and Exclusion Criteria

As the goal of the larger project within which this scoping review falls is to begin the process of assessing the evidence base for public policy or practice related to cybercrime, the decision was made to focus solely on studies in which research had been conducted. We define 'research' in this context as an empirically grounded, systematic study to identify, explain, predict

and/or determine the causes of a given phenomenon. For full details, Figure 1 below offers a visual presentation of our complete exclusion and inclusion criteria.

Figure 1. Visual Presentation of the Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Contains results of a research study	Does not contain discussion of a study (i.e., opinion piece, commentary)
Focus is on some aspect of Canadian public policing in the online environment	Focus is not on some aspect of Canadian public policing
Published in English	Is not published in English
Contains clear description of methodology employed	No discussion of research methodology employed
Conducted by a Canadian researcher	Inability to access paper

Coding and Analysis

To answer the first and second research questions, we employed a simple inductive coding scheme using the following categories: title, first author, year of publication, topic, approach (quantitative, qualitative, or mixed methods), methods (data collection and analysis techniques),

and data source. Answering the third research question required a novel approach. We had to construct a list of topics that were potentially missing from the Canadian literature. To do this, we relied upon the published annual meeting program guides of the American Society of Criminology (ASC) annual conferences. As the ASC hosts one of the largest international criminology conferences, it can be deduced that the program agendas would reflect some of the major concerns and interests in the field of cybercrime generally and cyberpolicing more specifically. To develop our list, we searched each of the program guides available (2005 to 2021) for paper titles and abstracts and then coded relevant abstracts. The results are located in Appendix III. Finally, to achieve a measure of reliability in the coded data, all coding was independently verified.

Findings

Extent and Range of the Literature

As can be seen in Table 1 below, prior to 2010, we were only able to locate three studies: one (n=1) peer-reviewed article (2008), one (n=1) report from Statistics Canada (2002) and one (n=1) Master's Thesis (2009). After 2008, a six-year gap emerged in which we could find no relevant peer-reviewed Canadian literature and only a handful of studies produced in the form of academic theses or dissertations. The lack of research in this area began to shift in 2014, with scholars publishing, on average, one peer-reviewed paper per year. Scholarly output in the form of theses and dissertations occurred randomly across both decades. We could only locate one (n=1) government report from 2002 and nothing beyond that date.

Table 1. Crosstabulation of the Year and Number of Works Located (2001-2021)

Year	Journal Articles	Reports, Theses, and Dissertations	Total
2001	0	0	0
2002	0	1	1
2003	0	0	0

2004	0	0	0
2005	0	0	0
2006	0	0	0
2007	0	0	0
2008	1	0	1
2009	0	1	1
2010	0	0	0
2011	0	1	1
2012	0	0	0
2013	0	0	0
2014	1	0	1
2015	1	0	1
2016	1	0	1
2017	1	0	1
2018	1	0	1
2019	2	1	3
2020	3	1	4
2021	1	1	2
Total	**12**	**6**	**18**

While the overall volume of Canadian research on cyberpolicing and related topics is fairly low, we did observe some diversity in terms of the types of research methods employed. In particular, studies were almost evenly split between quantitative (n=7) and qualitative methods (n=8), with only one mixed methods study combining survey and interview data. Qualitative studies relied heavily on interview data, whereas quantitative typically drew on secondary data and some primary data sources by way of surveys conducted by the researchers. We also note that much of the research – both quantitative and qualitative – was descriptive and exploratory in nature. One significant concern is the lack of experimental research, a method often used in evaluative studies. This finding suggests that what is missing from research in this area are studies assessing how well specific cyberpolicing programs, policies, and practices are performing in terms of meeting program or institutional objectives.

Table 2. Research Methods

Methodology	n
Quantitative	
Survey	3
Existing dataset	4
File review	1
Experimental	0
Qualitative	
Interviews	8
Content analysis	0
Focus groups	1
Experimental	0
Mixed methods	
Interviews	1
Survey	1

While policing tends to fall squarely within the field of criminology because of the technical and socially complex nature of cyber-crime and cyberpolicing, these topics are best thought of as inherently multi-disciplinary fields of study. To determine the extent to which the included studies reflected the multi-disciplinary nature of the field, we looked to the institutional affiliation of the first author. In doing so, what we observed is that all of the studies were produced by researchers working within the social sciences. Except for two studies – one by Statistics Canada (Kowalski 2002) and the other by the Canadian Policing Knowledge Network (Beesely 2021) – which are depicted under the 'general' disciplinary category, the remainder were largely within the domains of criminology (n=9), sociology (n=3) and legal studies (n=3). Interestingly, despite the fact that some of the studies examined explored psychological dimensions of cyberpolicing, only one study came from the field of psychology (n=1). Overall, cyber-crime and cyberpolicing emerged as explored within a total of eighteen (n=18) research domains (see Table 3). These spheres represent the disciplines/perspectives that are influencing empirics and assumptions and also expectedly driving public policy and practice.

Table 3. Scholarly Fields in Which the Research was Produced

Research Domain	n
Criminology	9
Sociology	3
Legal Studies	3
Psychology	1
Social Sciences (general)	2
Total	**18**

Given the international scope of the issue of cyber-crime, we expected to see Canadian researchers exploring issues related to the trans-jurisdictional nature of cyberpolicing, and thus some Canadian-focused studies that relied on the use of data from international sources. What we found is that the majority of studies used data from Canadian sources, including surveys of Canadian police services, interviews with Canadian police officers, and information collected by Statistics Canada (n=14). Only two papers – both on the effects of policing efforts on online illicit markets – contained international data (n=2).

In the eighteen (n=18) papers located, we identified twenty (n=20) discrete topics[1]. While there is a healthy diversity of topics covered within the Canadian literature, there are too few studies on any one topic to contribute to and develop a strong evidence base. As can be seen in Table 4 below, eighteen (n=18) of the topics appear in the literature fewer than five times, with ten (n=10) of these appearing only once.

If we had to identify the most frequently occurring topics, a loose definition would be appearing in the collected studies four or more times. Thus, our results would include three (n=3) topics: child sexual exploitation, police attitudes towards cybercrime and investigation. Of these, police work on 'child sexual exploitation' (CSE) was the most frequently occurring of all topics

---

[1] Some papers addressed more than one topic. Given this, we opted not to include a final total at the base of Table 4.

(n=7). This result can be explained by the fact that one research team (Spencer, Ricciardelli, Dodge et al. 2020) generated a single study on Internet Child Exploitation teams that contributed four papers. Sub-topics in these papers included: police resources, aspects of the police investigation, occupational stress and digital evidence. The other two papers similarly looked at CSE work with a sub-focus on issues related to digital evidence, technology, and occupational stress.

'Police attitudes' and aspects of investigational work appeared in five (n=5) papers each. Papers examining police attitudes towards cyber-related work were generally in the context of more significant explorations of CSE, cyberbullying and/or police resources for responding to cybercrimes. The topic identified as 'aspects of police investigation' – that is, looking at one or more investigational processes or outcomes – also appeared in relation to two papers on CSE, as well as in one paper on illicit online markets. 'Digital evidence' was one of these topics, notably found in papers on CSE, as we have stated above. This was also the case with 'police resources' with one exception: the issue of police services lacking sufficient personnel to deal with a particular type of offense also appeared in one paper on intellectual property (IP) theft. Police 'training' issues were also a more frequent topic (n=4).

In terms of frequency, the next group of topics were those that appeared in more than one paper but in fewer than four. Issues related to 'police data' – particularly the possibility of inaccuracies due to underreporting – were raised in three (n=3) papers. The topics of 'enforcement efforts' and 'online illicit markets' were identified in a pair of articles (n=2) on the effects of police 'crackdowns' on piracy and drug crypto sites. We also found two papers (n=2) on police involvement in preventing and/or responding to cyberbullying.

Our final cluster of topics was found in one paper (n=1) each. These included 'human trafficking,' 'public-private collaborations,' 'police prevention work,' 'technology issues,'

'occupational stress,' 'intellectual property theft,' 'working with victims,' and 'police searches' of seized technology. It is worth noting that, although a significant issue in Canada and elsewhere, research into police investigations of cyber-mediated forms of human trafficking has drawn little attention to date. This was also the case with two other important topics: police-led 'prevention measures' and police 'interactions with victims' of cyberharms. Unsurprisingly, given that digital evidence was a primary focus of three papers (n=3), related fields such as 'police searches' and 'technology issues' also appear at least once. Lastly, the issues of 'civilianization' of police roles in cyber-response and investigation, police 'digital competencies' (required skills for specific roles), and 'police recruitment' each appeared in one (n=1) paper.

Table 4. Topics Represented Within the Canadian Literature and Their Frequency

Topic	n
Child sexual exploitation	7
Police attitudes	5
Investigation	4
Digital evidence	4
Police resources	4
Police training/education	4
Police data	3
Enforcement efforts	2
Cyberbullying	2
Online illicit markets	2
Human trafficking	1
Public-private collaborations	1
Police prevention	1
Technology issues	1
Occupational stress	1
IP theft	1
Working with victims	1
Police searches	1
Civilianization of police roles	1
Police recruitment	1
Police digital competencies	1

Missing Topics

11

As will be recalled, to determine what topics might be missing from the Canadian research literature on cyberpolicing, we constructed a list based on topics in paper presentations at the ASC for the years 2005 to 2021[2]. The complete list of those identified by year can be found in Appendix I. We recognize there are significant limitations in this approach, not the least of which is that the list represents those subjects that have been studied and not a list of all possible topics. Thus, there are likely many, many more subjects we could include. That said, we offer this analysis as a starting point to a much more extensive discussion of possible avenues for future research.

Based on our review of the ASC presentations, we identified the following as topics missing from the Canadian research literature:

- information sharing across jurisdictions
- policing of hacking
- policing of romance scams
- comparing law enforcement approaches
- policing of cyberterrorism
- policing of online frauds
- policing of identity theft
- policing cyber-harassment
- gender (women in cyberpolicing) and
- local police responses to cybercrimes

Conclusions and Recommendations

As can be seen throughout this report, the overall volume of research in this area – both scholarly and in government reports – is low, averaging about one study per year. While we note a recent increase in volume (notably in 2020), constructing a strong evidence base to support cyberpolicing efforts will require initiative and investment from policymakers.

One area in which Canadian research is clearly lacking is the production of rigorous evaluative and experimental research into cyberpolicing and the effects of different cyberpolicing strategies. This means that we are not trialling new initiatives, and/or when police agencies

---

[2] There was no annual meeting held in 2020 due to COVID-19. Therefore, we used the agenda for the 2021 conference

implement new strategies or technologies, they are not being independently or rigorously assessed. Programs or policies aimed at improving the quality of policing in this area need to vigorously promote the benefits of this type of research to both scholars and police services.

An aspect of this research we were pleased to note is the range of topics covered. That said, we also identified ten topic areas of which we could locate no relevant Canadian research, and we are aware that our list of missing topics is hardly representative of the entire spectrum of issues that could be covered. Therefore, policy-makers and funding organizations should consider developing initiatives to help fill in many of these gaps.

Additionally, Canadian research on cyberpolicing is in a relatively healthy shape with respect to the use of diverse research methods and approaches. We are contributing to exploratory, descriptive and causal research through the use of quantitative and qualitative methods. Policymakers should continue to support different research approaches while pushing for the development of innovative and creative programmes of research.

Even though cybercrime and cyberpolicing are areas that lend themselves easily to multidisciplinary and interdisciplinary approaches, most of the studies identified for this report were produced within criminology or sociology departments. Policymakers and funding agencies should also encourage the growth of research that uses multiple disciplinary lenses. Doing so will help generate a stronger oeuvre of Canadian research and lead to a more vibrant community of researchers in this area.

Acknowledgements

Appendix I: List of Peer-Reviewed, Published Canadian Papers on Cyberpolicing Topics (2001-2021).

Baird, K., McDonald, K. and Connolly, J. 2020. 'Sex Trafficking of Women and Girls in a Southern Ontario Region: Police File Review Exploring Victim Characteristics, Trafficking Experiences, and the Intersection with Child Welfare.' *Canadian Journal of Behavioural Science / Revue Canadienne Des Sciences Du Comportement*, *52*(1), 8–17.

Broll, R. and Huey, L. 2015. '"Just Being Mean to Somebody Isn't a Police Matter": Police Perspectives on Policing Cyberbullying.' *Journal of School Violence*, 14(2): 55-176

Broll, R. 2016. 'Collaborative Responses to Cyberbullying: Preventing and Responding To Cyberbullying Through Nodes and Clusters.' *Policing and Society*, 26(7): 735-752

Burns, C., Morley, J., Bradshaw, R. and Domene, J. 2008. 'The Emotional Impact on And Coping Strategies Employed by Police Teams Investigating Internet Child Exploitation.' *Traumatology, 14*(2), 20–31.

Décary-Hétu, D. 2014. '*Police Operations 3.0*: On The *Impact And Policy Implications Of Police Operations On The Warez Scene*.' *Policy & Internet*, 6(*3*), 315–340.

Décary-Hétu, D., and Giommoni, L. 2017. 'Do Police Crackdowns Disrupt Drug Cryptomarkets? A Longitudinal Analysis of The Effects of Operation Onymous.' *Crime Law and Social Change,* 67(1): 55–75.

Dodge A. and Spencer, D. 2018. 'Online Sexual Violence, Child Pornography or Something Else Entirely? Police Responses to Non-Consensual Intimate Image Sharing among Youth.' *Social & Legal Studies*, 27(5):636-657.

Dodge A., Spencer, D., Ricciardelli, R., and Ballucci, D. 2019. "This Isn't Your Father's Police Force": Digital Evidence In Sexual Assault Investigations.' *Australian & New Zealand Journal of Criminology*, 52(4):499-515.

Popham, J., McCluskey, M., Ouellet, M. and Gallupe, O. 2020. 'Exploring Police-Reported Cybercrime In Canada: Variation and Correlates.' *Policing: An International Journal*, 43(1): 35-48.

Ricciardelli R., Spencer, D. and Dodge, A. 2021. '"Society Wants to See a True Victim": Police Interpretations of Victims of Sexual Violence.' *Feminist Criminology,*16(2):216-235.

Spencer, D., Ricciardelli, R., Ballucci, D. and Walby, K. 2020. 'Cynicism, Dirty Work, and Policing Sex Crimes.' *Policing: An International Journal*, 43(1): 151-165.

Watson, C. and Huey, L. 2020. 'Technology as a Source of Complexity And Challenge For Special Victims Unit (SVU) Investigators.' *International Journal of Police Science & Management*, 22(4):419-427.

Appendix II: List of Grey Literature on Cyberpolicing Topics (2001-2021)

Beesely, P. 2021. 'Competency-Based Management Framework for Digital Competencies In Canadian Policing.' Report of the Canadian Police Knowledge Network.

Dawson, C. 2009. 'Perspectives On the Capacity of The Canadian Police System to Respond To "Child Pornography" On the Internet.' Available at: https://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn000040047009-eng.pdf

Kowalski, M. 2002. 'Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics.' Available at: https://www.publicsafety.gc.ca/lbrr/archives/cnmcs-plcng/cn600-eng.pdf

Kusz, J. 2020. '"Obscenity Has Fallen to The Wayside": The Decline of The Obscenity Provisions Amongst Law Enforcement Professionals in Canada.' Available at: https://summit.sfu.ca/item/21070

Robertson, J. 2019. 'The Impact of the Digital Society on Police Recruit Training in Canada.' Available at: https://ir.library.dc-uoit.ca/bitstream/10155/1127/1/Robertson_James_G.pdf

Sutherland, D. 2011. 'Measuring The Response To Intellectual Property Crime in The Greater Toronto Area by The Royal Canadian Mounted Police.' Available at: https://www.collectionscanada.gc.ca/obj/thesescanada/vol2/002/MR76366.PDF

Appendix III: List of Topics Based on ASC presentations (2005[3]-2021[4]).

Notes:

Subjects in papers by Canadian scholars are denoted with an asterisk *
A paper could include more than one topic; each topic is listed separately

2005: digital evidence
2006: public-private collaboration, investigation
2007: police searches, police attitudes, public-private collaboration*
2008: investigation & information sharing across jurisdictions
2009: policing of hacking
2010: policing of cyberbullying, policing of romance scams, police cybercrime resources, comparing law enforcement approaches.
2011: public-private collaboration*, policing of CSE, occupational stress, police cybercrime resources, police investigation, technology issues
2012: policing of online human trafficking
2013: policing of cyberterrorism, police cybercrime resources
2014: policing of cyberterrorism, policing online frauds, police prevention strategies, police and victims, policing of identity theft
2015: digital forensics
2016: policing of CSE*, police investigation*
2017: policing cyber-harassment*,
2018: police cybercrime resources, civilianization,
2019: general officer views on cybercrime, gender (women in cyberpolicing), policing online illicit markets, issues with police cybercrime data
2021: interagency collaboration, police and cyber-prevention*, local police responses*, gender (women in cyberpolicing), investigation & information sharing across jurisdictions, policing online illicit markets*, police searches, police investigation*, policing of CSE*.

---

[3] 2005 is the first year in which the ASC made its program available online and searchable.
[4] There was no annual meeting held in 2020 due to the Covid-19 pandemic. We have, therefore, used the agenda for the 2021 conference

References

Arksey, H., and O'Malley, L. 2005. Scoping studies: towards a methodological framework. *International journal of social research methodology*, *8*(1), 19-32.

Royal Canadian Mounted Policy [RCMP]. 2021. New cybercrime and fraud reporting system. Available at: https://www.rcmp-grc.gc.ca/en/new-cybercrime-and-fraud-reporting-system.

Sherman, L. W. 1998. *Evidence-based policing* (p. 15). Washington, DC: Police Foundation.

Sherman, L. W., Farrington, D. P., Welsh, B. C., and MacKenzie, D. L. (Eds.). 2002. Evidence-based crime prevention. New York: Routledge.