

**THE UNITED NATIONS DRAFT CONVENTION AGAINST CYBERCRIME IN THE
CANADIAN CONTEXT: A PURPOSEFUL APPROACH**

by

PRAIRIE MORGAN

*A thesis submitted in partial fulfilment of
the requirements for the degree of*

BACHELOR OF ARTS (HONOURS)

in

CRIMINAL JUSTICE

*We accept this thesis as conforming
to the required standard*

Honours Thesis Supervisor

Doug King
Professor

Department of Economics, Justice, and Policy Studies

MOUNT ROYAL UNIVERSITY



**MOUNT ROYAL
UNIVERSITY**
1910

© **Prairie Morgan**
Calgary, Alberta, Canada

TABLE OF CONTENTS

TABLE OF CONTENTS	i
DECLARATION	v
Notice One	v
Notice Two	v
ABSTRACT	vi
LAND ACKNOWLEDGEMENT	vii
ACKNOWLEDGEMENTS	viii
CHAPTER I: INTRODUCTION	1
Chapter Overview	1
Background.....	1
Research Question	2
Rationale and Significance	3
Rationale	3
Significance.....	3
Scope and Structure	3
Chapter Summary.....	3
CHAPTER II: LITERATURE REVIEW	5
Chapter Overview	5
Convention Perceptions	5
Interpretation	7
Canada: Cybercrime and Human Rights	8
Interpretation	9

Convention Purview	10
Interpretation	11
UN Member States and Cyber Practice	11
People's Republic of China	13
Egypt	14
India	14
People's Democratic Republic of Korea	15
Russian Federation	16
Interpretation	17
Chapter Summary.....	18
CHAPTER III: THEORETICAL APPROACH	19
Chapter Overview	19
Overview of Theoretical Approach	19
Rationale for Using the Chosen Theoretical Approach	20
Contextual Analysis	21
Selection: Risks to Canada and Domestic Laws	21
Conclusion	22
CHAPTER IV: METHODOLOGY AND RESEARCH DESIGN	23
Chapter Overview	23
Overview of Methodological Approach	23
Description of Methodology	25
Collection and Analysis of Data	25
Collection	26

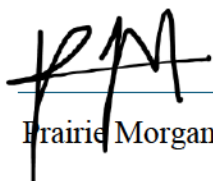
Analysis	27
Chapter Summary	27
CHAPTER V: DATA ANALYSIS AND RESULTS	29
Disclaimer	29
Chapter Overview	29
Theory	29
Purposive Analysis	30
Contextual Analysis	30
Textual Analysis	33
Addressing the Research Question	36
Research Question One	36
Sub-Question One	37
CHAPTER VI: DISCUSSION AND CONCLUSION	39
Implication and Recommendations	39
REFERENCES	41
APPENDIX	53
Legal Comparison Data	53
Cyber-Related Definitions	53
Identity and Personal Information	57
Illegal Access and Misuse	59
Illegal Interception and Interference	63
Forgery, Fraud, and Theft	67
Sexual Offences	71

Criminal Involvement	80
Liability, Adjudication, and Sanctions	84

DECLARATION

To the best of my knowledge and belief, this thesis contains no material previously published by any other person except where due acknowledgement has been made. This thesis contains no material which has been accepted for the award of any other degree or diploma in any university.

This thesis may be made available for loan and limited copying in accordance with the Copyright Act, RSC 1985, c C-42.



April 10th, 2025

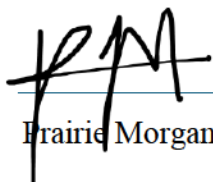
Date

Notice One

Under the Copyright Act, RSC 1985, c C-42, this thesis must be used only under the normal conditions of scholarly fair dealing. In particular no results or conclusions should be extracted from it, nor should it be copied or closely paraphrased in whole or in part without the written consent of the author. Proper written acknowledgement should be made for any assistance obtained from this thesis.

Notice Two

I certify that I have made all reasonable efforts to secure copyright permission for third-party content included in this thesis and have not knowingly added copyright-protected content to my work without the owner's permission.



April 10th, 2025

Date

Institutional Repository Statement

This thesis is deposited in the Mount Royal University Institutional Repository for long-term access and preservation. It is made available under the terms of the author's chosen license and is subject to institutional repository policies.

ABSTRACT

Following three years of negotiation, the United Nations approved the final draft of the Convention Against Cybercrime in late 2024. Canada is an active member of the UN and played a participatory role in the creation of the Convention. Cybercrime increased in Canada at the turn of the millennium and continued into the Covid-19 pandemic; some scholars argue that current policies unjustly limit Canadian rights under existing cybersecurity threats. This research examined the context of cybercrime in Canada and contrasted the criminal definitions in the Convention with the cyber practices in Canada and other Member States (China, Egypt, India, North Korea, and Russia). The purposive approach, a tool used in the adjudication of Charter cases in Canada, was used to facilitate an interpretation of the Convention that is sensitive to current conditions and flexible enough to support future applications. A contextual analysis was used to examine current cybercrime conditions and a textual analysis compared the definitions in Articles 2-21 to Canadian law. Few concerns were noted for Canadians or those in Canada. Possible risks to Canada's national security and the wellness of those outside of Canada were identified, especially in regard to human rights and fundamental freedoms. Canada will likely accept the Convention in late 2026. It is recommended that regulatory safeguards are enacted to ensure the security of Canadian data in collaborative cybercrime investigations with UN Member States.

LAND ACKNOWLEDGEMENT

Land Acknowledgements are traditional protocol to pay respect to the deeply interconnected relationship Indigenous peoples have with their hereditary lands.

This research was conducted at Mount Royal University, situated on Treaty 7 lands of the Niitsitapi (or Blackfoot) Nations of the Siksika, Kainai and Piikani; the Tsuu T'ina Nation; the Nakoda Nations of the Bearspaw, Chiniki and Wesley; and the Metis Nations. The agreements made between the ancestral peoples of this land and the first Euro-Canadian settlers have been historically dishonoured. In recognizing the legacy of my own Euro-Canadian ancestors, this Land Acknowledgement honours the past and present Indigenous peoples of Treaty 7; original keepers of the fresh air, clean water, and beautiful landscapes I am fortunate to be surrounded by.

ACKNOWLEDGEMENTS

This research was made possible by the ongoing support I received throughout my studies.

To my grandparents, David and Noreen Bailes, thank you for your love and encouragement. Your celebration of my achievements has motivated me through every class, shift, and setback.

To my research supervisor, Doug King, thank you for your guidance and words of promotion. The merits of this research are thanks to your supportive and flexible oversight.

The community at Mount Royal University has helped me grow through challenge and opportunity. The quality of my education is attributed to many kind, dedicated, and insightful staff. In particular, I would like to thank Dr. Kirsten Kramar, Dr. Christina Witt, and Leann Acheson of the Criminal Justice faculty; Lori Williams in Policy Studies; and Dr. Matt Murphy in Humanities (Philosophy).

CHAPTER I: INTRODUCTION

I-1) Chapter Overview

The purpose of this chapter is to illustrate the current state of cybercrime and cyber threats as experienced by Canadians and in reference to the UN's (United Nations) proposed cybercrime legislation. Information will come from existing sources. This overview is needed in order to critically examine international cybercrime legislation in the Canadian context.

An exploration of the thesis, research questions, and rationale for research will follow. Contextualizing the current state of cyber affairs with existing research on Canadian cyber trends will lay the groundwork for a purposive analysis between Canadian law for cyberspace with those prescribed by the proposed *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

I-2) Background

In 2023 it was estimated that organized cybercrime will threaten the Canadian economy and national defenses within the next two years (Canadian Centre for Cyber Security, 2023). The use of technology to advance geopolitical interests is rapidly increasing; state-sponsored cyberthreats already effect macro and micro levels of Canadian society. UN Member States such as China, North Korea, and Russia have previously threatened cyber defence strategies in Canada and present an ongoing risk to national security (Canadian Centre for Cyber Security, 2023). The social media algorithms of Canadians are commonly exploited with digitally-created disinformation in order to complicate public opinion and fulfill political agendas (Canadian Centre for Cyber Security, 2023). Between 2014 and 2022, the rate of online child pornography in Canada increased by 290% (Savage, 2024, Highlights).

As will be discussed with more depth in later sections, there is a gap in the collection of statistics pertaining to the prosecution of cybercrime and cyber-related offences in Canada. Police-reported data shows that, excluding for child pornography offences, 41% of cases involving online child sexual abuse were cleared by police in the last decade (Savage, 2024, Highlights). However, a performance audit in 2024 indicated that poor case management and incident tracking has limited the Royal Canadian Mounted Police's (RCMP) ability to respond to cyber incidents (Office of the Auditor General of Canada, 2024).

Efforts against cybercrime are exacerbated by the jurisdictional complexity of prosecuting internationally-operant cybercriminals. Legislative obstacles are common (Interpol, 2024). In an effort to strengthen international regulation and litigation, the UN negotiated the draft *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137)).

Cyber victimization is a risk to Canadians, organizations, and Canada itself. As a Member State of the UN, there is a pressing need to compare Canadian jurisprudence with Articles and definitions in the proposed *Convention* ahead of the signatory deadline on December 31st, 2026 (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

I-3) Research Question

RQ1: How do the offences in the United Nations Draft Convention against Cybercrime compare to Canadian legal definitions?

SQ1: Does the Convention pose a risk to Canadians?

I-4) Rationale and Significance

The purpose of this thesis is to contextualize Canadian cybercrime practice with the UN's draft *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). The constitutional protections outlined in the *Canadian Charter of Rights and Freedoms* are a priority to the administration of justice in Canada (*Canadian Charter of Rights and Freedoms* [Charter], Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11). Appreciating the *Convention's* possible influence on Canadian jurisdictions requires a comparison of domestic and international cyberspace (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137) .

Although the findings of this research are most pressing ahead of the signatory deadline, the data will continue to benefit future discourse on the legalities of cybercrime in Canada and the UN. As a founding Member State, Canada's fiduciary duty to the largest global intergovernmental organization will continue to evolve as new developments are made in cybercrime and policy.

I-5) Scope and Structure

The scope of this research is focused on Canadian sources. A variety of statistics and literature will be used to describe the existing political and criminal climate of cybercrime. Gaps in research are identified. A purposive analysis will only be performed for topics with sufficient existing information to support the process. The structure of this chapter offers a brief overview of the thesis, purpose, and theoretical framework of this study.

I-6) Chapter Summary

This chapter briefly summarizes existing data on cybercrime and anticipated threats in Canada in order to prime a critical reflection of the UN's proposed *Convention* (United

Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

It reviewed areas of concern for Canadian criminal justice and discussed the efficacy of local law enforcement.

CHAPTER II: LITERATURE REVIEW

II-1) Chapter Overview

This chapter will explore cybercrime, human rights, and the UN *Convention* within the context of Canada (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). 95% of Canadians fifteen or older used the internet in 2022 (Statistics Canada, 2023, Table 22-10-0135-01). The last three years have seen ransomware attacks on 6 Ontario hospitals, breaches to the personal information of military personnel and Government of Nova Scotia employees, and disrupted payments in the energy sector as a result of a cybersecurity incident (Canadian Centre for Cybersecurity, 2024). Threats to critical infrastructures pose a risk to all Canadians.

Strategies and resources to combat cybercrime grew exponentially following the Covid-19 pandemic (Canadian Anti-Fraud Centre, 2023). Law enforcement's predictive capabilities are weakened by the pace of digital and cybercriminal advancements; artificial intelligence (AI)-assisted cybercrime further complicate the issue (European Union Agency for Law Enforcement Cooperation, 2024).

II-2) Convention Perceptions

Extenuating measures seem intuitive provided the rapid growth of cybercrime. However, advocates have expressed hesitancy about the *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Advisors to the UN warned that Articles lacking a qualified form of intent may risk the criminalization of research and crime prevention (United Nations Human Rights Special Procedures, 2024). The scope of the *Convention* was also called into question; the investigation and collection of electronic data is

permitted for any offence subject to a punishment of four years or more, not just cybercrimes, under Article 35 (United Nations Human Rights Special Procedures, 2024).

Similar sentiments were echoed in a joint statement of over one hundred civil society groups with concerns ranging from improper safeguards for researchers and journalists to excessive data sharing with governments exercising significant deviance from international human rights standards (United Nations. Joint_statement of the proposed cybercrime treaty ahead of the concluding session (23, January 2024), SR OP8-OP9). Existing cybercrime legislation, the *Budapest Convention*, has been frequently referenced as evidence that an additional agreement is unneeded (Council of Europe, *Convention Against Cybercrime*, 23 November 2001, CETS No 185 (entered into force 1 July 2004)). The Council of Europe (2024) noted that there are enduring concerns regarding adequate safeguards in the *Convention* even after adjustments were made following recommendations that referenced international human rights standards (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). These concerns are cited in context to the political conditions of other Member States.

Human rights organizations have argued that the *Convention* could create hurdles for prosecutors and loopholes for child pornography offenders under Articles 14, 15, and 16 (Centre for Family & Human Rights, 2024; United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Most notably, the definition of child pornography in the UN's *Optional Protocol* varies from possible definitions in the *Convention* (*Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography* [Optional Protocol], GA Res 54/263, UNGAOR, 54th Sess, UN Doc A-27531 (entered into force 25 May 2000) vol. 2171). The former defines child pornography as any

representation, by whatever means of but not limited to, any representation of the sexual parts of a child primarily for sexual purposes (*Optional Protocol*, 2000, at art. 2(c)), while the latter allows for exclusions of non-visual content or material that does not depict an existing person (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137 at art. 15).

Other sources have welcomed the adoption of the first legally binding international agreement for cybercrime. Interpol (2024) praised the integration of existing cybersecurity solutions into the *Convention*, further citing a long overdue need for a framework that strengthens international cooperation (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). The United States (US) delegation to the UN addressed humanitarian concerns by citing Articles 6, 24, and 40 as written safeguards and further noted that any requests made for the purpose of human rights abuses will not be executed (Shrier, 2024). Canada accepted the Second Additional Protocol and held domestic consultations to inform stakeholders on the *Convention* (Government of Canada, 2024f; United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

II-2-a) Interpretations

As argued by the US, Member States have the ability to dispute and deny requests that risk the wellness of human rights. This is further supported by Articles in the *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Nevertheless, safeguards should be considered in context to what they are intended to defend. With electoral democracy on the decline in 2024, an increasing number of Member Parties exercise governmental practices that are inconsistent with respect for human rights and fundamental freedom (Valgarosson et al., 2025).

II-3) Canada: Cybercrime and Human Rights

Canada serves as a Party to seven international human rights conventions and acknowledges that all nations have a duty to promote human rights under international law (Government of Canada, 2024b). Internet freedom, pluralism and diversity, the protection of human rights defenders, women and girls, and children and youth were identified as factors of focus in 2024. Canada provides support for legal training, practical assistance, and the development of democratic systems to assist other nations in meeting their commitments to international human rights standards (Government of Canada, 2024b). The Universal Periodic Review (UPR), a council that evaluates each Member State's respective human rights standards on a rotational basis, was championed by Canada ahead of its introduction in 2008 (Government of Canada, 2017). The UPR facilitates international discourse by allowing Member States to review findings and make recommendations based on the report. Canada has and continues to take an international approach in an effort to advance global freedom (Government of Canada, 2024b).

The Government of Canada has demonstrated an awareness of the *Convention's* potential impact on gender equality. Multiple defences were made in favour of a gender mainstreaming approach to international cyber policy in a submission to the proposals third amendment, with suggests for Article Preventative Measures (Article 53) and Technical assistance and Capacity building (Article 54) (*Report of the Ad Hoc Committee to elaborate a comprehensive international Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on its reconvened concluding session*, UNGA, 78th Sess, (August 19, 2024) UN Doc A/AC.291/26). A gender mainstreaming approach is present in the proposal's Preamble but the recommendations are not present in the Articles they were submitted

under (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

Some scholars have argued that a lack of legal clarity in cyberspace, legitimate government secrecy in national security operations, and policy laundering have hindered or degraded Canada's legislative safeguards against the collection of cyber intelligence (Ogasawara, 2022; Arnell & Faturoti, 2022). Canada signed the first international cybercrime legislation, the *Budapest Convention*, in 2001 (Government of Canada, n.d; Council of Europe, *Convention Against Cybercrime*, 23 November 2001, CETS No 185 (entered into force 1 July 2004)). Compliance with the *Budapest Convention* and policies favouring national security have been cited as legitimizing increased surveillance and intelligence sharing in Canada, despite impairments to established legal standards for Canadian privacy (Ogasawara, 2022; Bennett et al., 2014).

II-3-a) Interpretations

Ongoing cyber diplomacy illustrates Canada's eagerness to strengthen international cooperation in cyberspace (Global Affairs Canada, 2023; Government of Canada, 2023; Global Affairs Canada, 2020b). Canada's interest in forming and maintaining strong international relations is likewise well-demonstrated. Frequent participation in international discourse gives Canada the opportunity to address concerns and facilitate the protection of human rights on the global stage. With such a heavy focus on domestic and international liberties, the Government of Canada also has a responsibility to ensure that diplomatic actions are balanced in respect to the rights of Canadians and the global political atmosphere. In comparison to aid or support, international agreements have a greater impact due to the associated changes in domestic legislation and potential effects on citizens outside of Canada.

II-4) Convention Purview

It is important to note that Member States have an obligation to fulfill and implement the orders of the *Convention* if it is signed (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Articles for criminal offences carry an onus to collect evidence, investigate, and bring justice to cited offences. Article 47 governs State Parties to cooperate closely with one another in combating cybercrime, including the expedited exchange of information related to the location and identity of suspected offenders (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137 at art. 47). International cooperation and mutual legal assistance clauses include requests for the preservation, seizure, and access of electronic and traffic data (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137 at art. 42-46). Various Articles also require a consistency between accepted standards for human rights and applications of the proposal (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Clauses to protect fundamental freedoms are also present in addition to requirements to obtain informed consent prior to extradition (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-141376, at art. 6; 40).

II-4-a) Interpretations

Interjurisdictional collaboration increases the efficacy of law enforcement (Legrand & Leuprecht, 2021). Collaborative success is contingent on the commitment of involved parties to meet shared objectives. In terms of the draft *Convention*, many Articles have optional clauses or considerations for domestic law (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-141376). Provided there are 193 members affiliated with the United Nations, the possible application and scope of the *Convention* should be considered in

context to the varying legal ideologies of Party Members (United Nations, n.d; United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-141376).

II-5) UN Member States and Cyber Practice

Human rights advocates have accused numerous governments of misusing cybercrime legislation to advance political agendas. A possible tool to evaluate the political positions of UN Member States is Article 6. The second paragraph states,

Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law. (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137, at art. 6)

The Ad Hoc committee for the *Convention* voted on a proposal to remove this clause (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-141376). The motion was brought to the committee by the Islamic Republic of Iran.

The votes were as followed:

In Favour:

Burkina Faso, Central African Republic, Chad, Democratic People's Republic of Korea, Egypt, India, Iran (Islamic Republic of), Iraq, Jordan, Libya, Malaysia, Mali, Mauritania, Nicaragua, Niger, Oman, Russian Federation, Sudan, Syrian Arab Republic, Venezuela (Bolivarian Republic of), Yemen, Zambia, Zimbabwe.

Against:

Albania, Algeria, Andorra, Angola, Antigua and Barbuda, Argentina, Armenia, Australia, Austria, Bahamas, Bangladesh, Barbados, Belgium, Bolivia (Plurinational State of), Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Canada, Chile, Colombia, Costa Rica, Côte d'Ivoire, Croatia, Cyprus, Czechia, Denmark, Dominican Republic, Ecuador, El Salvador, Estonia, Fiji, Finland, France, Georgia, Germany, Ghana, Greece, Grenada, Guatemala, Guyana, Haiti, Honduras, Hungary, Iceland, Ireland, Israel, Italy, Jamaica, Japan, Kiribati, Lao People's Democratic Republic, Latvia, Lebanon, Liechtenstein, Lithuania, Luxembourg, Malawi, Malta, Mauritius, Mexico, Monaco, Montenegro, Mozambique, Namibia, Nepal, Netherlands (Kingdom of the), New Zealand, Norway, Palau, Panama, Papua New Guinea, Paraguay, Peru, Philippines, Poland, Portugal, Republic of Korea, Romania, Rwanda, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, San Marino, Sao Tome and Principe, Serbia, Slovakia, Slovenia, South Africa, Spain, Sri Lanka, Suriname, Sweden, Switzerland, Thailand, Tonga, Trinidad and Tobago, Tunisia, United Kingdom, United States, Uruguay, Vanuatu.

Abstained:

Bahrain, Belarus, Benin, Botswana, Brunei Darussalam, Cameroon, China, Cuba, Djibouti, Eritrea, Gambia, Indonesia, Kenya, Morocco, Nigeria, Pakistan, Qatar, Saudi Arabia, Senegal, Sierra Leone, Singapore, Togo, Türkiye, Uganda, United Republic of Tanzania, Viet Nam. (United Nations General Assembly, *Report of the Ad Hoc Committee to elaborate a comprehensive international Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on its reconvened concluding session*, (19 August, 2024), 78th Sess, UN doc. A/AC.291/26)

The vote failed. However, it may lend credence to the concerns cited by human rights advocates.

II-5-a) People's Republic of China

Cybersurveillance is a primary method of governance and social control in China; internet search platforms are subject to over 60 000 censorship parameters and authorities frequently instruct service providers to unpublish user's content (Human Rights Watch, n.d.-a, Freedom of Expression). China has executed extra-legal renditions of Hong Kong booksellers as punishment for those accused of damaging the state's reputation, which Canada acknowledged in a statement regarding China's 2017 *National Intelligence Law* (Government of Canada, 2018). Clauses include the punishment of individuals or organizations identified as problematic. A clear separation exists for the collection of data between military personnel and civilians (Government of Canada, 2018).

The Canadian Cyber Threat Assessment established China's aggressive cyber program as the most active and sophisticated cyber threat to Canada between 2025 and 2026 (Canadian Centre for Cyber Security, 2024). Global cyber espionage, surveillance, and cyberattack capabilities were cited as primary concerns. Critics of the Chinese Communist Party (CCP) in Canadian governments are particularly vulnerable to cybersecurity threats and Chinese surveillance (Canadian Centre for Cyber Security, 2024). Uyghur minority members in Canada have been victimized by Chinese espionage operations that relied on spyware and spear phishing schemes (using spoofed or counterfeit digital communications against specific victims in an attempt to access sensitive information, such as usernames or passwords) (Canadian Centre for Cyber Security, 2024).

II-5-b) Egypt

In 2018, Egypt ratified the *Anti-Cyber and Information Technology Crimes* law (Sadek, 2018). Uploading original content to social media or other websites that violate Egyptian principles and family values can carry a fine and or a minimum of six months in prison (Mada Masr, 2018). This could include various forms of free speech and advocacy, such as discussing women's reproductive rights. The same legislation includes a minimum of one year imprisonment and or a fine for those who, whether intentionally or not, access or hack a website, personal account, or prohibited information system (Mada Masr, 2018).

Two-way trade between Canada and Egypt totalled \$1.252b in 2023 (Government of Canada, 2024a). Amongst strengthening trade ties the Canadian government has noted key issues in the international relationship. Freedom of expression, association, and the rights of women and girls were noted areas of interest in supporting the nation promote democratic governance, pluralism, and human rights (Government of Canada, 2024a). Canada has previously sent a recommendation to Egypt under the UPR citing the need to take action in the protection of lesbian, gay, bisexual, transgender, queer, and intersex (LGBTQI) individuals against discriminatory arrest or prosecution (Government of Canada, 2021b).

II-5-c) India

India's *Information and Technology Act*, 2000, Act No 21/2000 (June 9th, 2000), s 69A permits restriction on public access to any information through any computer resource. This legislation was used to restrict access to 7502 accounts and websites by the Indian Parliament in 2023 (Freedom House, n.d.-a). Government agencies in India were accused of using spyware to conduct targeted surveillance on the cell numbers and WhatsApp accounts of journalists, politicians, and activists; in 2021, the Supreme Court of India ordered a probe into the

investigation (Amnesty International, 2023). Internet and telecommunication blackouts are frequently executed by Indian government officials. Justifications include response to protests, cheating in school or government employer exams, and violence (Freedom House, n.d.-a). Muslim-majority cities Jammu and Kashmir were without internet and telecommunications services for eighteen months between 2019 and 2020 as a result of state concerns about extremism in the area (Human Rights Watch, 2023; Hussain, 2023). The blackouts were cited as collective punishment that is inconsistent with legal proportionality in a joint statement by the UN (Human Rights Watch, 2023).

Assessments made by the Canadian Centre for Cybersecurity (2024) indicate that Indian state actors are likely to conduct espionage through cyberthreats in Canada. The same report notes that new developments in India's cyber program provide a means to advance national security imperatives; motivations were linked to the promotion of India's global status and countering critical views of the state. Indian cybercriminals have also targeted Canada. A pro-Indian hacktivist group claimed to infiltrate the public Canadian Armed Forces website following an accusation by the Canadian government that India was involved with the killing of a Canadian citizen (Canadian Centre for Cybersecurity, 2024).

II-5-d) People's Democratic Republic of Korea

With an authoritarian government that systemically controls all personal liberties, North Korea is one of the most repressive countries worldwide (Human Rights Watch, n.d.-b). There are severe consequences for North Koreans who access unsanctioned phones, computers, radio, or media. Most citizens are not permitted to access the internet; the dissemination of digital information occurs through a state-sponsored intranet (a computer network that facilitates internal communication without external access) (Human Rights Council, 2014). An inquiry into

human rights in North Korea noted that the punishment for watching South Korean soap operas was execution by gunshot or ten to fifteen years in a prison camp (Human Rights Council, 2014).

Malicious cryptocurrency software has been used by North Korean cyber actors to obtain credentials and steal funds from Canadian individuals and organizations (Canadian Centre for Cybersecurity, 2022a). It is theorized that criminal proceeds are used to fulfill political and military objectives. The Canadian government has stated that although North Korea does not seriously threaten domestic national security, there is a persistent risk of state-sponsored cybercrime against Canadian organizations and individuals (Government of Canada, 2022a; Canadian Centre for Cyber Security, 2024).

II-5-e) Russian Federation

After sharing a YouTube video that detailed atrocities against Ukraine by Russia's military, Russian politician Ilya Yashin was sentenced to over eight years in prison (European External Access Service, 2022). Roskomnadzor, the federal agency responsible for the censorship of media and telecommunications in Russia, requires internet service providers to register under the state; in 2018, the Federal Security Service of the Russian Federation (FSB) mandated the installation of equipment that provides immediate access to decryption keys for private telecommunications (Human Rights Watch, 2020). This is despite an existing bill, the *Yarovaya* law, which permits complete oversight of internet services by FSB officials and requires service providers to surrender digital data upon request (Moyakaine & Tabachnik, 2021). The *Yarovaya* bill is subject to judicial measures; the 2018 changes by the FSB are not.

Russian-led cyberattacks and disinformation operations increased in Canada following a military response to Russia's invasion of Ukraine, (Government of Canada, 2024e). Similar

threats are a shared concern for many North Atlantic Treaty Organization (NATO) members (Canadian Centre for Cybersecurity, 2022a). Estimating the actual extent of Russian cybersecurity threats is difficult in respect to the numerous cybercriminal and hacktivist groups that have claimed support for the Russian cause following the recent war (Canadian Centre for Cybersecurity, 2022a). The Government of Canada (2024e) has warned that an extended exposure to Russian disinformation online risks polarizing the opinion of Canadians and undermining trust in democratic institutions.

II-5-f) Interpretation

Canada's international relations are complicated. Many factors beyond the scope of justice moderate Canada's relationship to the global community, such as economic, political, and cultural ties. Salient to these complexities is the wellness and security of Canadians. As will become apparent in the *Convention* analysis, telecommunications services and systems often subsume the personal information of the user (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Service operation is subject to local legislative boundaries and legal definitions. Interjurisdictional translations, such as international law enforcement operations on cybercrime, require some degree of legal synonymity.

Cybercrime attacks and legal discrepancies with nations involved in the *Convention* are a cause for concern (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Depending on the degree of deviation from international human rights standards, effective cybercrime cooperation with some nations seems unachievable. Denying information requests could carry retaliative political penalties. Nevertheless, cybercrime continues to pose a variable risk to Canada, our allies, and adversaries. Given the

interjurisdictional nature of cybercrime, a suitable method of combat will likely rely on international collaboration.

II-6) Chapter Summary

The UN's draft *Convention* has important objectives (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). An international standard for cybercrime justice increase collaboration and provide law enforcement agencies with parameters for acceptable cyber operations. The inclusion of human rights clauses and limitations on authority further insulate the benefits of the proposal.

Creating a functional standard for an evolving issue is complex. Cybercriminals can innovate faster than the UN can review, hear, and pass motions. Political inconsistencies between Member States are likely to complicate collaborative processes and challenge the safeguards of the *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Relying on strict internal policies, as suggested by the United States, may be unreliable; turbulent political conditions are an ongoing concern for various Member States and may arise unexpectedly for others. Evidence that was previously shared with a different ruling party may become compromised in the hands of another. Canada's acknowledgement of state-sponsored cyberattacks and surveillance by members of the UN further illustrates the risks associated with the proposed legislation.

CHAPTER III: THEORETICAL APPROACH

III-1) Chapter Overview

This Chapter covers a review of the theoretical approach for this thesis. Existing perspectives in the Literature Review were guided by a contextual analysis that will inform a purposive analysis of the *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). A thorough investigation of existing global attitudes and statistics allowed the theoretical framework to remain grounded in Canada while simultaneously identifying relevant international affairs. Justification for the choice of Literature Review sources will also be provided in order to better situate the theoretical context of this thesis.

III-2) Overview of Theoretical Approach

The theoretical framework for this thesis mimics the purposeful approach used in Canadian jurisprudence. Purposeful analysis is typically reserved for interpretations of the *Charter*; it considers the intended purpose of a right in context to Canada's constitutional protections, stressing the need for an approach that is broad enough to accommodate developments over time (*Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11). This will be a useful lens to examine the draft *Convention* in Canada because an analysis of the Articles will likewise require an interpretation of their purpose and possible applications (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

A central tenet of the purposeful approach is the liberal interpretation of rights and freedoms for those in Canada. Canada is fortunate to have a judiciary that is critical of police overreach and protective of established liberties. This is not the case for all Member States of the

UN. In anticipation of possible legal exploitation, a purposeful analysis will be used to interpret rights in the *Convention* as well as the scope of law enforcement. In Canadian courts, the state is burdened with justifying limitations on rights (*Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, s 1). This is critical to the purposive approach. Legal impairments to constitutional protections need to be demonstrably justified in a free and democratic society. Given the security against infringement in Canada and Canada's commitment to advancing human rights abroad, the burden of justification is an important consideration in context to the *Convention* and possible limitations on individual rights in cyberspace (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

The Canadian judiciary sometimes complements purposeful analysis with other legal tools (Government of Canada, 2024c). Two are relevant to this thesis. A textual analysis relies solely on the written content of the law and uses wording to suggest meaning; a contextual analysis considers the social, political, and legal context of the issue at law and may be used to find a balance between individual and social interests.

III-3) Rationale for Using the Chosen Theoretical Approach

A purposeful analysis allows for a generous interpretation that is steered by current conditions and future developments. While the draft *Convention* is comparatively micro to the constitutional nature of the *Charter*, the international scope of the United Nations requires a flexible interpretation for legislation (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137; *Canadian Charter of Rights and Freedoms* [Charter], Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK),

1982, c 11). Understanding the global milieu of cyberspace is crucial in order to make Canadian-informed abstractions about the proposed agreement.

III-3-a) Contextual Analysis

A contextual analysis was the guiding lens of the Literature Review. This ensured a diverse perspective that is sensitive to international conditions and Canada's relationship with UN Member States. Moreover, it provides foundational context to further inform the implication of legislative variance between Canadian law and the draft *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). *Charter* cases allow the courts to hear from interveners; in addition to the frequent reference of Canadian sources, this was mimicked by the reference of many nonprofit and civil society organizations in the Literature Review (*Canadian Charter of Rights and Freedoms* [Charter], Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11). Additions from historic allies, such as the United States and European Union, further contributed to contextualizing *Convention* perspectives with relevance to Canada (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

III-3-b) Selection: Domestic Laws and Risks to Canada

Article 6 was selected as a comparative tool because Canada has closely aligned itself with a commitment to human rights. Member States were selected for a contextual analysis based on identification in Canada's 2025-2026 cyber threat assessment or frequent reference by advocates against the *Convention* (in addition to concerns cited by Canada), specifically Egypt. A review of UN Member States domestic rule on cybercrime alludes to their national ideologies; this will strengthen later interpretations in the purposeful analysis. For the same purpose, the human rights offences of Member States and state-sponsored cybercrime against Canada were

discussed. A review of current crimes and policies is useful in the approximation of future applications for the proposal.

III-4) Conclusion

This chapter explored the core principles of the purposive analysis and translated its framework from Canadian jurisprudence to the proposed *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). An explanation and application of the purposive approach's contextual analysis was used to justify the selection and interpretation of sources in the Literature Review. A wide net was cast to include *Convention* perspectives from interveners on human rights, Canada's historic partners, and Canadian sources (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). This replicates the generous interpretation of the purposive analysis by taking consideration for the document in question, in this case the draft *Convention*, and the international scope in which it applies (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

CHAPTER IV: METHODOLOGY AND RESEARCH DESIGN

IV-1) Chapter Overview

The research methodology of this thesis relied on mixed qualitative approaches. In line with the purposive approach in Canadian jurisprudence, a literature review was used to provide an understanding of cybercrime and international policy in a Canadian context. A textual analysis followed in order to identify policy variations between the draft *Convention* and Canadian laws, as represented in the Appendix. This approach was used in order to produce a data analysis that adheres to the purposive framework.

This chapter discusses specifics of the purposive method and justification for its use.

IV-2) Overview of the Methodological Approach

A narrative scoping literature review was used to discuss existing perceptions of global cybercrime and Canadian cybersecurity. Mozilla Firefox, Google Scholar, and the Mount Royal University Library database were used to identify critical sources. This topic is largely dominated by governments and civil society organizations; no sources were found with restricted access. Keywords used included the title of the proposed Treaty OR the title of a Member State with “Canada,” “Government of Canada,” “cyber,” “cybercrime,” “cyber policy,” “cybersecurity,” “human rights,” “internet,” “internet freedom,” and “surveillance.” Snowball sampling was used to further examine content where additional sources or elaboration was necessary to contextualize the literature in Canada.

In part, this literature review was limited by the researcher’s restriction to sources in the English language; while non-English sources were sometimes found they were excluded due to a lack of certainty in using online translation systems. The impact of this limitation is moderated by the prevalence of English language sources, especially those strongly connected to the

Canadian context. Selective and snowball sampling are limited in scope and at risk of researcher bias; this was overcome as much as possible by cross-referencing international claims with numerous sources for accuracy and objectivity. Sources from the Government of Canada were not cross-referenced; another possible limitation of this research is found in the working assumption that information made available by Canadian governments is reliable, correct, and fair. This is not to suggest that the Government of Canada is an idealistic institution, rather, making that evaluation extends beyond the scope of this research.

The textual analysis used in the comparison of *Convention* clauses and Canadian law was guided by the Articles selected for this thesis, 2-21 (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137, at art. 2-22). The effectiveness of textual analysis is limited to what can be interpreted from written words. However, its use does not purport to accomplish anything further; it is a tool of the purposive approach and works in tandem with other methods, such as contextual analysis, to provide a foundation prior to interpretative abstraction.

The Literature Review offered a comprehensive understanding of the nature of cybercrime and policy in Canada and other UN Member States. There is a gap in Canadian statistics for the prosecution of cybercrime or telecommunications-enabled crime. Existing data was sufficient to support an overview of cited concerns to the *Convention*, cybercrime and cybersecurity threats in Canada, Member State and domestic Canadian policy, and cybercrime in context to international human rights (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

IV-3) Description of Methodology

Legal analysis in Canada uses mixed-methods. Purposive analyses of *Charter* protections use textual and contextual analysis to inform judicial interpretation (*Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11). The proposed UN *Convention* demonstrates a similar need for a flexible and generous interpretation (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). The governance of cyberspace is likely to evolve as areas of exploitation are identified and amendments to existing practices are made. To apply the purposive method to the *Convention*, an analysis of Canada's international cybercrime affairs was conducted and then followed by a textual analysis of Canadian law with the draft *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

The selection criteria was targeted to Canada although snowball sampling was used to offer further insight. Cross-reference to global sources limited confirmation bias. Perceptions of the *Convention* were guided by Member States with a notable relationship to Canada; notable relationships were identified by Canada's grey literature on cybercrime, organizations that closely align with Canada's approach to human rights, and strong political ties (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Sources that made specific reference to the *Convention*, the international context of cybercrime and policy, the use of cyberspace to violate human rights, and cybercrime in Canada were included (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

This design was inspired by the protection of rights and freedoms in the Canadian judiciary. As a relatively new criminal domain unfolds, the governance of cyberspace becomes increasingly relevant. National and civil security should not unduly risk the right to reasonable limitations. Resolutions for an issue spanning nearly every jurisdiction possible is, self-evidently, quite challenging. Continued attention is needed in order to better inform the users, policy-makers, and advocates of cyberspace.

IV-4) Collection and Analysis of Data

IV-4-a) Collection

The primary methodology of data collection for this thesis was a narrative scoping literature review. It was initially guided by a search of critical positions relative to the proposed *Convention* and then further supported by snowball sampling (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Data was primarily collected from unrestricted grey literature with some additions from open source journals. Sources that preceded the year 2000, were not in English, or had unclear connections to the Canadian context were excluded. Although lightly limited by the inclusion criteria of this thesis, scoping reviews allow for a balanced approach to broad topics. Findings were further explored under a narrative framework as required by the purposive approach.

The Canadian legislation that governs cybercrime and cyberspace is relatively limited, so Article definitions were referenced against the Canadian *Charter*, *Criminal Code*, *Telecommunications Act*, *Personal Information Protection and Electronic Documents Act*, *Canada Evidence Act*, and *Foreign Interference and Security of Information Act* (Canadian *Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11; *Criminal Code*, RSC 1985, c C-46; *Telecommunications*

Act, SC 1993, c. 38; *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5; *Canada Evidence Act*, RSC 1985, c C-5; *Foreign Interference and Security of Information Act*, RSC 1985, c. O-5). For definitions with weak Canadian translations, the topic title or keywords were entered into an aforementioned search engine or database with “Canada law,” “Canadian,” and “Canada policy” to check for additional legislation or jurisprudence.

Researching the context of cybercrime in Canada with a Canadian analysis framework under the supervision of a Canadian institution inherently risks a conflict of interest. Decentralizing data sources away from the Government of Canada with additions from civil society organizations and other national governments mediated this as reasonably as possible. Like all academic research in Canada, the collection of data for this thesis was subject to the policies and guidelines of the Research Ethics Board (REB).

IV-4-b) Analysis

The analysis of data for this research included a detailed examination of literature in preparation for the contextual and textual analyses used to inform the purposive analysis. The purposive framework guided the synthesis of data into thematic categories of textual or contextual relevance, wherein applicable methods of interpretation were used.

The collection of data for this thesis relied on a broad scope of sources to acknowledge the complexity of international legislation. Although centralized to the Canadian context, additional perspectives about the draft *Convention* and international cybercrime were reviewed for a holistic approach that is sensitive to the global conditions of cyber policy (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

IV-5) Chapter Summary

This chapter covered an in-depth explanation of the methodological approach and data collections implemented in the development of this thesis. A narrative scoping review followed by contextual and textual analyses informed an examination of existing cybercrime policy in Canada and other UN Member States.

CHAPTER V: DATA ANALYSIS AND RESULTS

Disclaimer:

The purpose of the *Convention* is valuable (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). The protection of people and states in cyberspace relies on legal regulation and consequence. Moreover, Canada's international relationships are complex. Diplomacy is more than policy. National partners of today may become a threat to Canada's cybersecurity tomorrow. Likewise, state actors with a criminal hand against Canada may change course in the future. International relations should be considered in context to a functional and united succession.

V) Chapter Overview

This chapter discusses the results and theory of the analyses followed by a purposive interpretation. Existing perceptions of the *Convention* will be summarized (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

V-1) Theory

Above all, it is clear that cybercrime is a shared concern. Whether or not actions are taken with consideration for civil liberties, cybercrime is a growing area of policy for UN Member States. The abstract nature of cyberspace jurisdiction has historically complicated efforts for law enforcement to effect justice. At the same time, various state actors are accused of denying human rights in cyberspace; regulating cybercriminals should not prescribe an undue cost to fundamental freedoms.

V-2) Purposive Analysis

The purpose of the draft *Convention* is to facilitate international collaboration in the prevention and combat of cybercrime (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). As defined by the *Convention* itself, cooperation is required to control of cybercrime in the international domain (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Productive international policy is closely tied to the stability of state relations. Benefitting from the *Convention* relies on a combined effort from Member States and their respective government organizations (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). A generous consideration of the proposal should be sensitive to the current landscape of cybercrime both functionally and politically.

V-2-a) Contextual Analysis

The UN was formed with the intent of strengthening international connections in the promotion of peace and justice. The organization provides an opportunity for leaders to meet with the global community on various topics. This thesis is not at all positioned to make criticisms about the UN; diplomatic dialogue is an important objective and appears well-fulfilled by the organization. However, it is relevant to note that the UN does not itself have an enforcement unit. Member States carry the onus to self-regulate in accordance with international policy. The duty to condemn or intervene wrongdoings rests with each Member State, often with support from other Member States. Military disparities inherently create some imbalance; more powerful nations are less easily swayed by the threat of sanctions or interference.

Canada is an active member of the UN and an outspoken advocate on the importance of global human rights. Canada's peacekeeping has extended to the draft *Convention* with an

acceptance of the Second Additional Protocol and formal recommendations to uphold gender equality within the *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). This progress may be relative; research on Canadian cyber practices suggest that an overuse of surveillance and encroachments on privacy have been slowly legitimized in Canada following the acceptance of the *Budapest Convention* in 2001 (Ogasawara, 2022; Bennett et al., 2014; Council of Europe, *Convention Against Cybercrime*, 23 November 2001, CETS No 185 (entered into force 1 July 2004)). Moreover, suggestions for a gender mainstreaming approach are not present in the final *Convention* proposal (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

Eased intelligence sharing, synthesized law enforcement operations, and other benefits of the proposal are contingent on the willingness of other Member States to accept Canada's objectives in cyberspace (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). While many Parties to the UN share a relatively similar political ideology to Canada, many do not. The foreword of the Universal Declaration of Human Rights states that the international community has a duty to uphold the practices outlined in the document. It is inconsistent with the principles of international human rights standards to reject or abstain from voting on Article 6 of the *Convention* (UNGAOR, *Universal Declaration of Human Rights*, GA Res 217A (III), 3rd Sess, Supp No 13, UN Doc A/810 (1948) 71; United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). China abstained, while Egypt, India, North Korea, and Russia voted to have it removed. The Egyptian government has used internet technology to advance abuses on human rights, including the right to free speech. The other listed nations pose an ongoing risk to Canadian cybersecurity

through state-sponsored actors and political radicalism. Apart from the actual *Convention*, various Member States have a well-evidenced criminal interest in Canada, Canadian intelligence, and Canadians (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). UN negotiations have further highlighted a limited interest in ensuring the *Convention's* consistency with international human rights standards by the aforementioned nations (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

Cited concerns have largely focused on the draft *Convention* in context to the wider demographic in which it is proposed to operate (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). The Council of Europe (2024) made it clear that better safeguards are needed specifically due to the position taken by some Member States on human rights. This has translated into concern for the security of journalists, researchers, and advocates; there is significant variation in the protection of fundamental rights such as the freedoms of press, information, and speech worldwide (Alexander, 2024). The existing *Budapest Convention* was frequently referenced to guide the proposed *Convention* which, for some, has called into question whether additional legislation is necessary (Council of Europe, *Convention Against Cybercrime*, 23 November 2001, CETS No 185 (entered into force 1 July 2004); United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). The presence of optional clauses for sexual offences has also received significant attention. Child protection organizations have been particularly outspoken about Articles 14, 15, and 16, citing potential interjurisdictional conflicts for law enforcement and flexibility with child exploitation material produced with AI as needless limitations to the criminalization of child exploitation (Centre for Family & Human Rights, 2024).

There has also been significant support for the *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Interpol worked closely with the UN during the *Convention's* conception to ensure the legislation would be functional for law enforcement (Interpol, 2024). The organization also stated an overdue need for a legally binding international agreement on cybercrime (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). The United States stated that previous concerns about the *Convention* were addressed, further noting that its implementation is especially important to combat the disproportionate victimization of women and girls with the nonconsensual distribution of intimate images (Shrier, 2024; United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Robust domestic safeguards were cited as defence against concerns relating to other Member States, although it was also made clear that the *Convention* itself does not permit the suppression of human rights.

V-2-b) Textual Analysis

Convention definitions and offences are structured in a tabled comparison in the Appendix (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Descriptions are contrasted and evaluated based on their wording as guided by the textual analysis technique. Interpretations are made to discuss the scope of similarities and differences in context to Canada's legal practices. Subjects and respective laws are compared as defined by UN or Canadian law in accordance with the purposive approach's textual analysis. Topics are organized by legal subject matter. A discussion of variation follows each topic.

Many Articles and definitions in the *Convention* have comparable translations to existing Canadian laws (United Nations, *Draft United Nations convention against cybercrime*, (7 August

2024), vol. 24-14137). It is worth noting that Canada often demonstrated laws that were more definitive than those in the *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). It is likely however that a broad approach was necessary in context to the number of Member States the *Convention* will govern (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

Cyber-related definitions saw very little functional variation. Personal and identity information had only one notable clause, Subscriber Information (iii) (Appendix, Personal Identity and Information). While the limitations of a service agreement do serve as a safeguard the wording is exceptionally broad. Search and seizure, particularly in a residence or private business, is heavily regulated in Canada. Service agreements that exploit the quality of *Charter* s. 8 protections would not be legally enforceable (*Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, s 8). However, whether all Member States will exercise domestic protections to reasonably preserve the right to privacy is questionable at best.

Offences related to illegal access, interception, and interference were slightly less cohesive. The option to withdraw the requirement for dishonest or criminal intent in Article 7 (illegal access) risks criminalizing legitimate activities; an individual without right may not have criminal objectives, such as whistleblowers (Appendix, Illegal Access and Misuse). Although it can be reasonably forecasted that Canada will not opt out of 7(2), Parties that do could stunt cooperation between domestic law enforcements (Appendix, Illegal Access and Misuse). In contrast, Article 8 (Illegal Interception) has a section for the optional application of dishonest or criminal intent but Canada has no such requirements for unauthorized use or the interception of private communications (Appendix, Illegal Interception and Interference). A discrepancy may

occur in Articles 9 and 10 (inference offences) because Canada does not criminalize damage to essential infrastructure if it was incurred as a result of protest; it is very unlikely that less tolerant Member States have similar stipulations (Appendix, Illegal Interception and Interference).

Article 11 (Misuse of Devices) (3), reserves the right for Member States to determine whether it is criminal to make programs or devices for criminal use (Appendix, Illegal Access and Misuse)., The probative value of allowing the production of criminal tools is unclear in context to the objective of combating cybercrime.

The variations in offences related to theft, forgery, and fraud are limited to the application of Article 12 (2) (Appendix, Forgery, Fraud, and Theft). Canada has a stricter limitation on rights for forgery; the act is criminalized regardless of intent. The Article also includes data that is not intelligible without reference to specifics although it can be reasonably inferred to include encrypted data or data which becomes encrypted upon input. Considering the use of common digital tools offers a more flexible definition than what is currently present in Canadian law.

Sexual offence Articles deviate most significantly from Canadian law, especially in reference to optional clauses. Member States may choose to exclude the criminalization of child exploitation material that does not depict visual content or an existing person, sexual material that is taken by and for the private use of minors, grooming through digital communications without an act of furtherance, and nonconsensual distribution of intimate images without criminal intent (Appendix, Sexual Offences). These standards are inconsistent with Canadian policies that protect children and Canadians from sexual exploitation. Younger victims often serve as an aggravating factor in Canadian sexual offences (Appendix, Sexual Offences). In contrast, some *Convention* subsections can be combined in order to define offenses against older minors as intimate images rather than child exploitation material (Appendix, Sexual Offences;

United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). This classifies the offence as victimizing an adult rather than a child.

Criminal involvement saw little difference apart from one year of variation between Canada's definition of serious offences and the UN's slightly stricter definition of serious crime. Criminalized association in Article 17(b)(i) references association to a criminal offence, not an individual or identifiable group, and is therefore not a concern for human rights (Appendix, Criminal Involvement). The *Convention's* broad approach to liability, adjudication, and sanctions allows for a domestic lead (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). In Canada, aggravating circumstances are considered by the judiciary in order to facilitate a better understanding of an offence in context to which it occurred.

V-3) Addressing the Research Question

RQ1: How do the offences in the United Nations Proposed Treaty on Cybercrime compare to Canadian legal definitions?

Especially in terms of a textual analysis, most of the definitions in Articles 2-21 have a largely synonymous counterpart in Canadian law. Variation primarily occurs as a result of optional clauses that permit Member States to limit criminalization. This is most apparent in Articles governing sexual offences, 14, 15, and 16 (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137, at art. 14-16). If all optional clauses are engaged so as to limit criminalization, the scope and intensity of Canadian law is markedly more strict. Canada also takes a firmer stance against forgery and the production of devices for criminal use. In contrast, Canadian law is also more likely to require criminal intent, have exclusions for acts of protest, and provide definitions for legal terms (such as unintelligible

data in the *Convention*) (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

SQ1: Are there risks posed by the Treaty to Canadian Charter rights?

Even on balance, the risks of this *Convention* are relative to many factors beyond the document itself (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Taken as a whole without any optional measures to limit criminalization, the *Convention* is fairly cohesive with existing Canadian law; very few modifications would need to be made in order to adopt it (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). With that said, a significant portion of the Articles include optional clauses. The potential for domestic discrepancy in legislative applications is extremely high, especially in context to the political positions of some Member States.

Even though the draft *Convention* seems unlikely to truly facilitate effective cooperation amongst all Party members, the risk to those in Canada is probably quite low (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Requests from other Member States to the Canadian government will be subject to the usual safeguards for fundamental freedoms in Canada; it seems unlikely that Canada would facilitate an investigation or provide evidence for an act that is criminalized in another nation but a protected right in Canada. However and with great emphasis, this assumption relies on the Canadian justice system working as it is intended to. This is not always the case; law enforcement can overreach and judicial decisions are sometimes reversed or modified. The efficacy of safeguards for Canadian rights against international agreements are therefore directly related to the efficacy of the domestic system. In theory this is a very high standard. In practice it is open to error.

An enduring concern is also present in cybersecurity attacks that target multiple Member States; data sharing with Parties responsible for state-sponsored acts against Canada may be necessary if a cybersecurity threat affects both members because the *Convention* enforces collaborative investigations (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Whether this will translate into exploitations of the *Convention*, such as sponsoring a cyberattack and then fraudulently posing as a victim to gain intelligence, is in the very least a possibility (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

Concerns for Canadians travelling abroad are moderated by the pre-existing risks of domestic governance; an individual is always subject to local laws. The draft *Convention* does not itself pose a risk that a government could not otherwise enforce locally (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137).

VI: DISCUSSION AND CONCLUSION

VI-1) Implication and Recommendation

Canada is likely to sign the draft *Convention* in 2026 (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). At the individual level, it is probable that the impact to Canadians will be negligible. A textual analysis of the definitions within the proposal revealed that most of the Articles have a synonymous translation to Canadian law. The contextual analysis had more complex findings. Canadian cybersecurity risks, Member State cybercrime governance, and human rights in cyberspace are active factors in the consideration of the *Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Entering a legally binding agreement with Member States exercising a significant deviance from international standards for human rights should be done with caution. Optional clauses limit the likelihood of comparable frameworks. Even with an identical framework, the method of interpretation from one judiciary to another will likely differ; Canadian courts evidently have a different approach than Justices in North Korea.

The urgency to regulate cyberspace should not come at the expense of fundamental freedoms. The *Convention* in itself does not appear to pose any undue risk to Canadians or human rights; Member States responsible for offences against human rights are unfortunately likely to fulfill that agenda regardless of international regulations (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). However, the *Convention* also does not appear to be strictly necessary in light of existing cybercrime legislation, the *Budapest Convention* (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137; Council of Europe, *Convention Against Cybercrime*, 23 November 2001, CETS No 185 (entered into force 1 July 2004)). Even though

the *Budapest Convention* is not legally binding, the enforcement of the UN cannot necessarily ensure that Member States act in accordance with the proposed *Convention* either (Council of Europe, *Convention Against Cybercrime*, 23 November 2001, CETS No 185 (entered into force 1 July 2004); United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137). Moreover, the UPR provides an opportunity for Member States to engage in reflective discourse, including issues related to cybercrime and human rights in cyberspace (although opportunities are intermittent).

Threats to national security appear to be the greatest risk associated with the proposal. This thesis is unqualified to evaluate the nature of such risks nor the efficacy of Canada's national defences. The limited examination of law enforcement that was conducted suggests that more training is needed for RCMP officers responding to cybercrime. A lack of statistics related to Canadian cybercrime prosecution was a notable gap discovered during the collection of data.

The Convention will likely receive Canada's signature. To ensure the protection of Canadians and Canadian data, collaborative cybercrime investigations with Members States should be subject to thorough safeguards, oversight, and review. The advocacy of human rights is a strength in Canadian cybercrime affairs. Continued discourse and research is needed in Canada to support a proportional relationship between international justice and domestic security in cyberspace.

References

- Alexander, F. (2024). *UN threatens internet freedom, privacy, and due process*. Centre for European Policy Analysis. <https://cepa.org/article/un-threatens-internet-freedom-privacy-and-due-process/>
- Amnesty International. (2021). Forensic methodology report: How to catch NSO group's Pegasus. <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>
- Amnesty International. (2023). *India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists*. <https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/>
- Arnell, P. & Faturoti, B. (2022). The prosecution of cybercrime— why transnational and extraterritorial jurisdiction should be limited. *International Review of Law, Computers & Technology*, 37(1), 29-51. <https://www.tandfonline.com/doi/epdf/10.1080/13600869.2022.2061888?needAccess=true>
- Bennett, C. J., Haggerty, K. D., Lyon, D., & Stevens, V. (2014). *Transparent lives: Surveillance in Canada*. Edmonton: AU Press, Athabasca University. https://www.aupress.ca/app/uploads/120237_99Z_Bennett_et_al_2014-Transparent_Lives.pdf
- Canadian Anti-Fraud Centre. (2023). *Annual report 2022*. Government of Canada. https://publications.gc.ca/collections/collection_2024/grc-rcmp/PS61-46-2022-eng.pdf

Canadian Centre for Cybersecurity. (2022a). *Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine*. Government of Canada.

<https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf>

Canadian Centre for Cybersecurity. (2022b). *National cyber threat assessment 2023-2024*.

Government of Canada. <https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf>

Canadian Centre for Cybersecurity. (2023). *Baseline cyber threat assessment: Cybercrime*.

Government of Canada. <https://www.cyber.gc.ca/en/guidance/baseline-cyber-threat-assessment-cybercrime>

Canadian Centre for Cybersecurity. (2024). *National cyber threat assessment 2025-2026*.

Government of Canada. <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf>

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11.

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W.-J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security*, 105, 102258-. <https://doi.org/10.1016/j.cose.2021.102258>

Centre for Family & Human Rights. (2024). *Five problems with the UN cybercrime Treaty*.

https://c-fam.org/policy_paper/five-problems-with-the-un-cybercrime-treaty/#:~:text=Five%20Problems%20with%20the%20UN%20Cybercrime%20Treaty

Council of Europe, *Convention Against Cybercrime*, 23 November 2001, CETS No 185 (entered into force 1 July 2004).

Council of Europe. (2024). *United Nations treaty on cybercrime agreed by the Ad Hoc Committee*. <https://www.coe.int/en/web/cybercrime/-/united-nations-treaty-on-cybercrime-agreed-by-the-ad-hoc-committee>

Draft United Nations convention against cybercrime, United Nations, 7 August 2024, A/Ac.291/L.15. [Convention], online: <https://documents.un.org/doc/undoc/ltd/v24/055/06/pdf/v2405506.pdf>

Egyptian Front for Human Rights. (2025). *Privacy under attack: Egypt must reform its draft Criminal Procedure Code*. <https://egyptianfront.org/2025/02/privacy-under-attack-egypt-must-reform-its-draft-criminal-procedure-code/>

Epifanova, A. (2025). Throttling of YouTube shows that Russia is getting better at online censorship. Carnegie Politika. <https://carnegieendowment.org/russia-eurasia/politika/2025/02/russia-youtube-block-attempt?lang=en>

European External Access Service. (2022). *Russia: Statement by the spokesperson on the sentencing of politician Ilya Yashin*. European Union. https://www.eeas.europa.eu/eeas/russia-statement-spokesperson-sentencing-politician-ilya-yashin_en

European Union Agency for Law Enforcement Cooperation. (2024). *Internet organized crime threat assessment*. Europol. <https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf>

Freedom House. (n.d.-a). *India: Key developments, June 1, 2023 – May 31, 2024*. <https://freedomhouse.org/country/india/freedom-net/2024>

Freedom House. (n.d.-b). *Freedom on the net 2023: Russia*.

<https://freedomhouse.org/country/russia/freedom-net/2023>

Foreign Interference and Security of Information Act, RSC 1985, c. O-5.

Global Affairs Canada. (n.d.). *Project profile — Countering North Korean cyber security*

threats. <https://w05.international.gc.ca/projectbrowser-banqueprojets/project-projet/details/p012569001>

Global Affairs Canada. (2020a). *Canada expresses concern over pattern of malicious cyber activity by Russian Military Intelligence*. Government of Canada.

<https://www.canada.ca/en/global-affairs/news/2020/10/canada-expresses-concern-over-pattern-of-malicious-cyber-activity-by-russian-military-intelligence.html>

Global Affairs Canada. (2020b). *Canada welcomes European Union's announcement of new*

cyber sanctions listings. Government of Canada. <https://www.canada.ca/en/global-affairs/news/2020/07/canada-welcomes-european-unions-announcement-of-new-cyber-sanctions-listings.html>

Global Affairs Canada. (2023). *Chair statement: International discussions on collective responses to malicious cyber activity*. Government of Canada.

<https://www.canada.ca/en/global-affairs/news/2023/06/chair-statement-international-discussions-on-collective-responses-to-malicious-cyber-activity.html>

Government of Canada. (n.d.). *Convention on Cybercrime, Budapest, 23 November 2001*.

<https://www.treaty-accord.gc.ca/details.aspx?id=104677>

Government of Canada. (2017). *The Universal Periodic Review process*.

https://www.international.gc.ca/world-monde/issues_development-

[enjeux_developpement/human_rights-droits_homme/upr-eup/processus.aspx?lang=eng](https://www.international.gc.ca/world-monde/issues_developpement-enjeux_developpement/human_rights-droits_homme/upr-eup/processus.aspx?lang=eng)

Government of Canada. (2018). *China's intelligence law and the country's future intelligence competitions*. <https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html#fn67>

Government of Canada. (2021a). Criminal offences. <https://www.justice.gc.ca/eng/cj-ip/victims-victimes/court-tribunaux/offences-infractions.html>

Government of Canada. (2021b). *Egypt - Universal Periodic Review*. https://www.international.gc.ca/world-monde/issues_developpement-enjeux_developpement/human_rights-droits_homme/upr-eup/egypte-egypte.aspx?lang=eng

Government of Canada. (2022a). *Canada-Democratic People's Republic of Korea Relations*. https://www.international.gc.ca/country-pays/democratic_peoples_republic_korea-republique_populaire_democratique_coree/relations.aspx?lang=eng

Government of Canada. (2022b). *Evaluation of the investigative powers for the 21st Century initiative*. <https://www.justice.gc.ca/eng/rp-pr/cp-pm/eval/rep-rap/2020/ip21c-pe21s/p5.html>

Government of Canada. (2023a). *International cyber policy*. https://www.international.gc.ca/world-monde/issues_developpement-enjeux_developpement/peace_security-paix_securite/cyber_policy-politique_cyberspace.aspx?lang=eng#a2

Government of Canada. (2023b). The human rights of lesbian, gay, bisexual, transgender, queer, 2-spirit and intersex persons. [https://www.international.gc.ca/world-](https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/rights_lgbti-droits_lgbti.aspx?lang=eng)

[monde/issues_development-enjeux_developpement/human_rights-droits_homme/rights_lgbti-droits_lgbti.aspx?lang=eng](https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/rights_lgbti-droits_lgbti.aspx?lang=eng)

Government of Canada. (2024a). *Canada-Egypt relations.*

<https://www.international.gc.ca/country-pays/egypt-egypte/relations.aspx?lang=eng>

Government of Canada. (2024b). *Canada's approach to advancing human rights.*

https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/advancing_rights-promouvoir_droits.aspx?lang=eng

Government of Canada. (2024c). *General principles for the interpretation and application of the*

Charter. <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/principles-principes.html>

Government of Canada. (2024d). *How Canadian organizations are navigating cyber security in*

2024. <https://www.getcybersafe.gc.ca/en/canadian-organizations-are-navigating-cyber-security-2024>

Government of Canada. (2024e). *Russia's use of disinformation and information manipulation.*

https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng

Government of Canada. (2024f). *Second Additional Protocol on*

cybercrime. <https://www.justice.gc.ca/eng/cj-jp/cyber/index.html>

Government of India, *Information and Technology Act* (2000), s. 69A.

Online: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_update_d.pdf

How you will be affected by the new cybercrime law: A guide. (2018, August 21). Mada Masr.

<https://www.madamasr.com/en/2018/08/21/feature/politics/how-you-will-be-affected-by-the-new-cybercrime-law-a-guide/>

Human Rights Council. (2014). *Report of the detailed findings of the commission of inquiry on human rights in the Democratic People's Republic of Korea*. United Nations.

<https://documents.un.org/doc/undoc/gen/g14/108/71/pdf/g1410871.pdf>

Human Rights Watch. (2016). Russia: 'Big Brother' law harms security, rights.

<https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights>

Human Rights Watch. (2018). Human rights in North Korea: June 2018 briefing paper.

<https://www.hrw.org/news/2018/06/05/human-rights-north-korea>

Human Rights Watch. (2020). *Russia: Growing internet isolation, control, censorship*.

<https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship>

Human Rights Watch. (2021). *Abuse of cybercrime measures taints UN talks*.

<https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks>

Human Rights Watch. (2022). *Russia: New restrictions for 'foreign agents.'*

<https://www.hrw.org/news/2022/12/01/russia-new-restrictions-foreign-agents>

Human Rights Watch. (2023). *"No internet means no work, no pay, no food:" Internet shutdowns deny access to basic rights in "Digital India."*

<https://www.hrw.org/report/2023/06/14/no-internet-means-no-work-no-pay-no-food/internet-shutdowns-deny-access-basic>

Human Rights Watch. (n.d.-a). *China: Events of 2023*. <https://www.hrw.org/world-report/2024/country-chapters/china>

Human Rights Watch. (n.d.-b). *North Korea: Events of 2022*. <https://www.hrw.org/world-report/2023/country-chapters/north-korea>

Human Rights Watch. (2024a). Egypt: Opposition leader imprisoned.

<https://www.hrw.org/news/2024/06/04/egypt-opposition-leader-imprisoned>

Human Rights Watch. (2024b). *Human Rights Watch's comments on the updated draft text of the UN Cybercrime Convention*.

https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP8/HRW_comments_on_Rev3_20240729.pdf

Hussain, B. (2023, February 11). *Kashmir registers highest number of internet restrictions globally*. Voice of America. <https://www.voanews.com/a/kashmir-registers-highest-number-of-internet-restrictions-globally-/6958516.html>

Information and Technology Act, 2000, Act No 21/2000 (June 9th,

2000). <https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdiibgfGhdgFHtyhRtMjk4NzY=>

Interpol. (2024). *INTERPOL welcomes adoption of UN convention against cybercrime*.

<https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-welcomes-adoption-of-UN-convention-against-cybercrime>

Joint statement on the proposed cybercrime treaty ahead of the concluding session [Joint Statement]. (2024, January 23).

https://www.hrw.org/sites/default/files/media_2024/02/Joint_Advocacy_Statement-UN_Cybercrime_Treaty-Jan24.pdf

LaRue, F. (2014). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. United Nations General Assembly.

https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Lee, D. (2017). North Korea's brutality laid bare: More UN Security Council members should impose sanctions on Pyongyang. Human Rights Watch.

<https://www.hrw.org/news/2017/12/11/north-koreas-brutality-laid-bare>

Legrand, T., & Leuprecht, C. (2021). Securing cross-border collaboration: transgovernmental enforcement networks, organized crime and illicit international political economy. *Policy & Society*, 40(4), 565–586. <https://doi.org/10.1080/14494035.2021.1975216>

Marczak, B., Scott-Railton, J., McKune, S., Razzak, B. A., & Deibert, R. (2018). Hide and Seek; Tracking NSO group's Pegasus Spyware to operations in 45 countries. Munk School of Global Affairs & Public Policy. <https://citizenlab.ca/2018/09/hide-and-see-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>

Marczak, B., Scott-Railton, J., Roethlisberger, D., Razzuk, A. B., Anstis, S., & Deibert, R. (2023). *Predator in the wires: Ahmed Eltantawy targeted with predator spyware after announcing presidential ambitions*. Munk School of Global Affairs & Public Policy. <https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/>

Moyakine, E., & Tabachnik, A. (2021). Struggling to strike the right balance between interests at stake: The 'Yarovaya', 'Fake news' and 'Disrespect' laws as examples of ill-conceived

- legislation in the age of modern technology. *The Computer Law and Security Report* 40(105512), e1-e13. <https://doi.org/10.1016/j.clsr.2020.105512>
- Office of the Auditor General of Canada. (2024). *Report 7: Combating cybercrime*.
https://www.oag-bvg.gc.ca/internet/docs/parl_oag_202406_07_e.pdf
- Office of the United Nations High Commissioner for Human Rights. (n.d.). *Information note: Human rights and the draft Cybercrime Convention*.
<https://www.ohchr.org/sites/default/files/documents/issues/civicspace/DRAFT-CYBERCRIME-CONVENTION.pdf>
- Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography*, GA Res 54/263, UNGAOR, 54th Sess (Vol 2171), UN Doc A-27531 (25 May 2000).
- Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5.
- Public Safety Canada. (2025). *Parliamentary Committee notes: Canada-India engagement on security*. Government of Canada. <https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20250226/06-en.aspx>
- Report of the Ad Hoc Committee to elaborate a comprehensive international Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes on its reconvened concluding session*, UNGA, 78th Sess, UN Doc A/AC.291/26 (2024).
- Rodriguez, K. (2024). *The UN General Assembly and the fight against the Cybercrime Treaty*. Electronic Frontier Foundation. <https://www EFF.org/deeplinks/2024/08/un-general-assembly-and-fight-against-cybercrime-treaty>

Sadek, G. (2018). *Egypt: President ratifies anti-cybercrime law*. Library of Congress.

[https://www.loc.gov/item/global-legal-monitor/2018-10-05/egypt-president-ratifies-anti-cybercrime-law/#:~:text=than%20two%20years.-\(Law%20No.,about%20US%241%2C672%E2%80%93%2C786\).](https://www.loc.gov/item/global-legal-monitor/2018-10-05/egypt-president-ratifies-anti-cybercrime-law/#:~:text=than%20two%20years.-(Law%20No.,about%20US%241%2C672%E2%80%93%2C786).)

Savage, L. (2024). *Online child sexual exploitation: A statistical profile of police-reported incidents in Canada, 2014 to 2022*. Statistics Canada.

<https://www150.statcan.gc.ca/n1/pub/85-002-x/2024001/article/00003-eng.htm>

Shrier, J. (2024). *Explanation of position of the United States on the adoption of the resolution on the UN Convention Against Cybercrime in UNGA's third committee*. United States Mission to the United States. <https://usun.usmission.gov/explanation-of-position-of-the-united-states-on-the-adoption-of-the-resolution-on-the-un-convention-against-cybercrime-in-ungas-third-committee/>

Statistics Canada. (2023). *Internet use by province and age group* [Table].

<https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=2210013501>

Statistics Canada. (2024a). *Impact of cybercrime on Canadian businesses, 2023*.

<https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm>

Statistics Canada. (2024b). *Police-reported cybercrime, by cyber-related violation, Canada (selected police services)* [Table].

<https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000101>

Statistics Canada. (2024c). *Police-reported hate crime and cybercrime, preliminary quarterly data, first and second quarter of 2024*. [https://www150.statcan.gc.ca/n1/daily-](https://www150.statcan.gc.ca/n1/daily-quotidien/241024/dq241024e-eng.htm)

[quotidien/241024/dq241024e-eng.htm](https://www150.statcan.gc.ca/n1/daily-quotidien/241024/dq241024e-eng.htm)

Telecommunications Act, SC 1993, c. 38.

UNGAOR, *Universal Declaration of Human Rights*, GA Res 217A (III), 3rd Sess, Supp No 13,
UN Doc A/810 (1948) 71

United Nations. (n.d.). *About us*. Retrieved January 14, 2025, from <https://www.un.org/en/about-us#:~:text=Member-,States,the%20current%20193%20Member%20States>.

*Report of the Ad Hoc Committee to elaborate a comprehensive international Convention on
Countering the Use of Information and Communications Technologies for Criminal
Purposes on its reconvened concluding session*, UNGA, 78th Sess, UN Doc
A/AC.291/26 (2024). <https://docs.un.org/en/A/AC.291/28>

Valgarosson, V., Jennings, W., Stoker, G., Bunting, H., Devine, D., McKay, Lawrence., &
Klassen, A. (2025). A crisis of political trust? *Global trends in institutional trust from
1958-2019. British Journal of Political Science*, 55(15), e1-e23.
<https://doi.org/10.1017/S0007123424000498>

Youth Criminal Justice Act, SC 2002, c. 1.

Appendix

Legal Comparison Data

Cyber-Related Definitions

UN Convention Against Cybercrime	Canadian Law
<p>Information and communications technology system:</p> <p>shall mean any device or group of interconnected or related devices, one or more of which, pursuant to a program, gathers, stores and performs automatic processing of electronic data</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 2).</p>	<p>Computer system:</p> <p>a device that, or a group of interconnected or related devices one or more of which,</p> <p>(a) contains computer programs or other computer data, and</p> <p>(b) by means of computer programs,</p> <p>(i) performs logic and control, and</p> <p>(ii) may perform any other function;</p> <p>(ordinateur)</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s. 342.1(2)).</p>
<p>Electronic data:</p> <p>Shall mean any representation of facts, information or concepts in a form suitable for processing in an information and communications technology system, including a program suitable to cause an information</p>	<p>Electronic Document:</p> <p>Means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device;</p>

<p>and communications technology system to perform a function</p> <p>Content data:</p> <p>shall mean any electronic data, other than subscriber information or traffic data, relating to the substance of the data transferred by an information and communications technology system, including, but not limited to, images, text messages, voice messages, audio recordings and video recordings</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 2).</p>	<p>It includes a display, printout or other output of that data.</p> <p>Data:</p> <p>Means representations of information or of concepts, in any form.</p> <p>(<i>Canada Evidence Act</i>, RSC 1985, c C-5, s 31.8).</p>
<p>Traffic Data:</p> <p>Shall mean any electronic data relating to a communication by means of an information and communications technology system, generated by an information and communications technology system that formed a part in the chain of communication, indicating the communication's origin,</p>	<p>Transmission Data:</p> <p>Means data that</p> <p>(a) relates to the telecommunication functions of dialling, routing, addressing or signalling</p> <p>(b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of</p>

<p>destination, route, time, date, size, duration or type of underlying service</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 2).</p>	<p>enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and</p> <p>(c) does not reveal the substance, meaning or purpose of the communication.</p> <p>Tracking Data:</p> <p>Means data that relates to the location of a transaction, individual or thing.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s. 487.011).</p>
<p>Service Provider:</p> <p>Shall mean any public or private entity that:</p> <p>(i) Provides to users of its service the ability to communicate by means of an information and communications technology system; or</p> <p>(ii) Processes or stores electronic data on behalf of such a communications service or users of such a service</p>	<p>Telecommunications Service:</p> <p>Means a service provided by means of telecommunications facilities and includes the provision in whole or in part of telecommunications facilities and any related equipment, whether by sale, lease or otherwise</p> <p>Telecommunications Service Provider:</p> <p>Means a person who provides basic</p>

<p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 2).</p>	<p>telecommunications services, including by exempt transmission apparatus</p> <p>Telecommunications Common Carrier:</p> <p>Means a person who owns or operates a transmission facility used by that person or another person to provide telecommunications services to the public for compensation.</p> <p>(<i>Telecommunications Act</i>, SC 1993, c. 38, s 2(1)).</p>
---	---

The cyber-related definitions in Canadian law and the *Draft Convention Against Cybercrime* are largely synonymous. Variations are negligible in terms of application. The parameters of a computer system are slightly more defined than information and communication technology systems. Electronic documents and data in Canada have more breadth than content and electronic data; output is included in the definition of documents and data includes any form of information. The UN excludes subscriber and tracking data in this definition. Likewise, Canada excludes the substance, meaning, or purpose of a communication from the definition of transmission data. Traffic data as defined by the convention does not make this exclusion but a similar outcome is produced after distinguishing between traffic and content data. Services are also subject to similar regulatory definitions. The ability to process or store data is functionally the same as including the means of telecommunications facilities and any related equipment.

Identity and Personal Information

UN Draft Convention Against Cybercrime	Canadian Law
<p>Personal Data:</p> <p>Shall mean any information relating to an identified or identifiable natural person (United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 2).</p>	<p>Personal Information:</p> <p>Means information about an identifiable individual <i>(Personal Information Protection and Electronic Documents Act, SC 2000, c. 5, s 2(1)).</i></p>
<p>Subscriber Information:</p> <p>Shall mean any information that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:</p> <p>(i) The type of communications service used, the technical provisions related there to and the period of service</p> <p>(ii) The subscriber’s identity, postal or geographical address, telephone or other access number, billing or payment information, available on the basis of the service agreement or arrangement</p>	<p>Telecommunications:</p> <p>Means the emission, transmission or reception of intelligence by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system <i>(Telecommunications Act, SC 1993, c. 38, s 2 (1)).</i></p> <p>Intelligence:</p> <p>Means signs, signals, writing, images, sounds or intelligence of any nature <i>(Telecommunications Act, SC 1993, c. 38, s 2 (1)).</i></p> <p>Information requirements:</p>

<p>(iii) Any other information on the site of the installation of communications equipment, available on the basis of the service agreement or arrangement</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 2).</p>	<p>The Commission may require a Canadian carrier</p> <p>(b) to submit to the Commission, in periodic reports or in such other form and manner as the Commission specifies, any information that the Commission considers necessary for the administration of this Act or any special Act.</p> <p>(<i>Telecommunications Act</i>, SC 1993, c. 38, s 37 (1)(b)).</p> <p>Identity Information:</p> <p>(For the purposes of sections 402.2 and 403), means any information — including biological or physiological information — of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including a fingerprint, voice print, retina image, iris image, DNA profile, name, address, date of birth, written signature, electronic signature, digital signature, user name, ... or password.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 402.1).</p>
--	---

Personal data and personal information are clearly mirrored. The Canadian *Criminal Code* does make further reference to personal information in relation to identity theft, citing passwords, usernames, electronic and digital signatures alongside biological identifiers such as DNA and fingerprints (*Criminal Code*, RSC 1985, c C-46, s 402.1). Both definitions hold similar properties for application. Although Subscriber Information (iii) seems particularly broad, access to on-site information is bound by the basis of the service agreement which serves as a limitation for law enforcement.

Illegal Access and Misuse

UN Draft Convention Against Cybercrime	Canadian Law
<p>Article 7: Illegal Access</p> <p>1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally, the access to the whole or any part of an information and communications technology system without right.</p> <p>2. A State Party may require that the offence be committed by infringing security measures, with the intent of obtaining electronic data or other dishonest or criminal intent or in relation to an information and communications technology system that is connected to another</p>	<p>Unauthorized Use of Computer:</p> <p>Everyone ... who, fraudulently and without colour of right,</p> <p>(a) obtains, directly or indirectly, any computer service;</p> <p>(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;</p> <p>(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or</p>

<p>information and communications technology system</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 2).</p>	<p>(b) or under section 430 in relation to computer data or a computer system; or</p> <p>(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c).</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s. 342.1(1)).</p>
<p>Article 11: Misuse of Devices</p> <p>1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:</p> <p>(a) The obtaining, production, sale, procurement for use, import, distribution or otherwise making available of:</p> <p>(i) A device, including a program, designed or adapted primarily for the purpose of committing any of the offences established in</p>	<p>Possession of Device to Obtain Unauthorized Use of Computer System or To Commit Mischief:</p> <p>Every person who, without lawful excuse, makes, possesses, sells, offers for sale, imports, obtains for use, distributes or makes available a device that is designed or adapted primarily to commit an offence under section 342.1 or 430, knowing that the device has been used or is intended to be used to commit such an offence, is</p>

<p>accordance with articles 7 to 10 of this Convention; or</p> <p>(ii) A password, access credentials, electronic signature or similar data by which the whole or any part of an information and communications technology system is capable of being accessed; with the intent that the device, including a program, or the password, access credentials, electronic signature or similar data be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention; and</p> <p>(b) The possession of an item referred to in paragraph 1 (a) (i) or (ii) of this article, with intent that it be used for the purpose of committing any of the offences established in accordance with articles 7 to 10 of this Convention.</p> <p>2. This article shall not be interpreted as imposing criminal liability where the obtaining, production, sale, procurement for use, import, distribution or otherwise making available, or the possession referred to in paragraph 1 of this</p>	<p>(a) guilty of an indictable offence and liable to imprisonment for a term of not more than two years; or</p> <p>(b) guilty of an offence punishable on summary conviction</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s. 342.2(1)).</p> <p>Computer Password:</p> <p>Means any computer data by which a computer service or computer system is capable of being obtained or used</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s. 342.1(2)).</p> <p>Intercept:</p> <p>Includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s. 342.1(2)).</p> <p>Possession:</p> <p>(3) For the purposes of this Act,</p>
--	--

<p>article is not for the purpose of committing an offence established in accordance with articles 7 to 10 of this Convention, such as for the authorized testing or protection of an information and communications technology system.</p> <p>3. Each State Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (ii) of this article.</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 2).</p>	<p>(a) a person has anything in possession when he has it in his personal possession or knowingly</p> <p>(i) has it in the actual possession or custody of another person, or</p> <p>(ii) has it in any place, whether or not that place belongs to or is occupied by him, for the use or benefit of himself or of another person; and</p> <p>(b) where one of two or more persons, with the knowledge and consent of the rest, has anything in his custody or possession, it shall be deemed to be in the custody and possession of each and all of them.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s. 3.1).</p>
--	---

The scope of access and unauthorized use of a computer are most compatible when the Article 7 (2) applies, which requires a dishonest or criminal intent. Access and obtaining are functionally the same. Translating misuse of devices with Canada's computer possession offences is difficult if Article 11 (3) is applied. The clause restricts making information synonymous with password or access credentials available for criminal use, but Member States reserve the right to determine whether it is criminal to make programs or devices for criminal use. If applied, Article 11 (3) of the Convention is inconsistent with 342.2 (1) of the Criminal

Code. Nevertheless, both laws have a comparable scope. Article 11 (2) specifically references legitimate forms of access that are not to be criminalized, while the Canadian comparative references those without lawful excuse.

Illegal Interception and Interference

UN Draft Convention Against Cybercrime	Canadian Law
<p>Article 8: Illegal Interception</p> <p>1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the interception, made by technical means, of non-public transmissions of electronic data to, from or within an information and communications technology system, including electromagnetic emissions from an information and communications technology system carrying such electronic data</p> <p>2. A State Party may require that the offence be committed with dishonest or criminal intent, or in relation to an information and communications technology system that is</p>	<p>Interception:</p> <p>Every person who, by means of any electro-magnetic, acoustic, mechanical or other device, knowingly intercepts a private communication is guilty of</p> <p>(a) an indictable offence and liable to imprisonment for a term of not more than five years; or</p> <p>(b) an offence punishable on summary conviction.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 184 (1)).</p>

<p>connected to another information and communications technology system</p> <p>(<i>Convention</i>, 2024, Art 8).</p>	
<p>Article 9: Interference with Electronic Data</p> <p>1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the damaging, deletion, deterioration, alteration or suppression of electronic data.</p> <p>2. A State Party may require that the conduct described in paragraph 1 of this article result in serious harm</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 9).</p>	<p>Mischief in relation to computer data:</p> <p>Everyone commits mischief who wilfully</p> <p>(a) destroys or alters computer data;</p> <p>(b) renders computer data meaningless, useless or ineffective;</p> <p>(c) obstructs, interrupts or interferes with the lawful use of computer data; or</p> <p>(d) obstructs, interrupts or interferes with a person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it.</p> <p>(5.1) Everyone who wilfully does an act or wilfully omits to do an act that it is their duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or computer data,</p>

	<p>(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or</p> <p>(b) is guilty of an offence punishable on summary conviction.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 430 (1.1), 430(5.1)).</p>
<p>Article 10: Interference with a Communications and Technology System</p> <p>1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the serious hindering of the functioning of an information and communications technology system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing electronic data.</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 10).</p>	<p>Prejudice to the Safety or Interest of the State:</p> <p>For the purposes of this Act, a purpose is prejudicial to the safety or interests of the State if a person ...</p> <p>(d) interferes with a service, facility, system or computer program, whether public or private, or its operation, in a manner that has significant adverse impact on the health, safety, security or economic or financial well-being of the people of Canada or the functioning of any government in Canada</p> <p>(<i>Foreign Interference and Security of Information Act</i>, RSC 1985, c. O-5, s 3 (1)).</p> <p>Sabotage — Essential Infrastructure:</p>

	<p>Every one ... who interferes with access to an essential infrastructure or causes an essential infrastructure to be lost, inoperable, unsafe or unfit for use with the intent to</p> <p>(a) endanger the safety, security or defence of Canada;</p> <p>(b) endanger the safety or security of the naval, army or air forces of any state other than Canada that are lawfully present in Canada; or</p> <p>(c) cause a serious risk to the health or safety of the public or any segment of the public</p> <p>(2) In this section, essential infrastructure means a facility or system, whether public or private, completed or under construction, that provides or distributes — or is intended to provide or distribute — services that are essential to the health, safety, security or economic well-being of persons in Canada, including the following: ...</p> <p>(b) information and communication technology infrastructure</p>
--	---

	(<i>Criminal Code</i> , RSC 1985, c C-46. s 52.1(1), 52.1(2)).
--	---

Canadian law does not include computer systems in reference to interception crimes, instead citing private communications. This is largely addressed within the unauthorized use of a computer. Article 8 (2) allows Member States to apply a requirement for dishonest or criminal intent. Canada does not have such a requirement for crimes relating to unauthorized use of a computer or interceptions of private communications. Interference with data is essentially equated with computer data mischief in Canada. Stipulations in Article 9 (2), which make it optional to require serious harm, are reflected in Canada's prejudice and sabotage laws that align with Article 10 of the Convention. Some discrepancy exists however; while Articles 9 and 10 state that acts are criminalized when committed intentionally and without right, Canada grants exception to acts against essential infrastructure, even if harm was incurred so long as it was not intended, if the objective was advocacy or protest under *Criminal Code* s 52 (5).

Forgery, Fraud, and Theft

UN Draft Convention Against Cybercrime	Canadian Law
Article 12: Information and Communications Technology System-Related Forgery 1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its	Forgery: Every one commits forgery who makes a false document, knowing it to be false, with intent

<p>domestic law, when committed intentionally and without right, the input, alteration, deletion or suppression of electronic data resulting in inauthentic data with the intent that they be considered or acted upon for legal purposes as if they were authentic, regardless of whether or not the data are directly readable and intelligible.</p> <p>2. A State Party may require an intent to defraud, or a similar dishonest or criminal intent, before criminal liability attaches.</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 12).</p>	<p>(a) that it should in any way be used or acted on as genuine, to the prejudice of any one whether within Canada or not; or</p> <p>(b) that a person should be induced, by the belief that it is genuine, to do or to refrain from doing anything, whether within Canada or not.</p> <p>(3) When Forgery Complete:</p> <p>Forgery is complete as soon as a document is made with the knowledge and intent referred to in subsection (1), notwithstanding that the person who makes it does not intend that any particular person should use or act on it as genuine or be induced, by the belief that it is genuine, to do or refrain from doing anything.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 366 (1), 366 (3)).</p>
<p>Article 13: Information and Communications Technology System-Related Theft or Fraud</p>	<p>Theft of Telecommunication Service:</p> <p>Every one commits theft who fraudulently, maliciously, or without colour of right ...</p>

<p>Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by means of:</p> <p>(a) Any input, alteration, deletion or suppression of electronic data;</p> <p>(b) Any interference with the functioning of an information and communications technology system;</p> <p>(c) Any deception as to factual circumstances made through an information and communications technology system that causes a person to do or omit to do anything which that person would not otherwise do or omit to do; with the fraudulent or dishonest intent of procuring for oneself or for another person, without right, a gain in money or other property.</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 13).</p>	<p>(b) uses any telecommunication facility or obtains any telecommunication service.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 326 (1)).</p> <p>Theft:</p> <p>Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything, whether animate or inanimate, with intent</p> <p>(a) to deprive, temporarily or absolutely, the owner of it, or a person who has a special property or interest in it, of the thing or of his property or interest in it;</p> <p>(b) to pledge it or deposit it as security;</p> <p>(c) to part with it under a condition with respect to its return that the person who parts with it may be unable to perform; or</p> <p>(d) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.</p> <p>Secrecy</p>
---	---

	<p>(3) A taking or conversion of anything may be fraudulent notwithstanding that it is effected without secrecy or attempt at concealment.</p> <p><i>(Criminal Code, RSC 1985, c C-46. s 322 (1), 322 (3)).</i></p> <p>Fraud:</p> <p>Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service</p> <p><i>(Criminal Code, RSC 1985, c C-46. s 380 (1)).</i></p> <p>Fraudulent Concealment:</p> <p>Every person who, for a fraudulent purpose, takes, obtains, removes or conceals anything is guilty</p> <p><i>(Criminal Code, RSC 1985, c C-46. s 341).</i></p> <p>False Pretence:</p> <p>A false pretence is a representation of a matter of fact either present or past, made by</p>
--	--

	<p>words or otherwise, that is known by the person who makes it to be false and that is made with a fraudulent intent to induce the person to whom it is made to act on it.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 361 (1)).</p>
--	---

Canadian forgery varies with notable significance from the Convention's definition, especially if the requirements of intent in Article 12 (2) are applied. Regardless of an intent to make use of it, a document is considered forged as soon as the act is complete in Canada. Article 12 includes data that is not intelligible but does not necessarily indicate what such data might be. Risk of exploitation is minimized in the same section by noting the act must be committed intentionally and without right. There are no notable discrepancies between theft or fraud in the *Convention* and Canadian law; the latter simply references more because it addresses both theft in general and theft as it pertains to communication technology.

Sexual Offences

UN Draft Convention Against Cybercrime	Canadian Law
<p>Article 14: Offences Related to Online Child Sexual Abuse or Child Sexual Exploitation Material:</p> <p>1. Each State Party shall adopt such legislative and other measures as may be necessary to</p>	<p>Making Child Pornography:</p> <p>Every person who makes, prints, publishes or possesses for the purpose of publication any child pornography is guilty of an indictable offence and liable to</p>

<p>establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <p>(a) Producing, offering, selling, distributing, transmitting, broadcasting, displaying, publishing or otherwise making available child sexual abuse or child sexual exploitation material through an information and communications technology system;</p> <p>(b) Soliciting, procuring or accessing child sexual abuse or child sexual exploitation material through an information and communications technology system;</p> <p>(c) Possessing or controlling child sexual abuse or child sexual exploitation material stored in an information and communications technology system or another storage medium;</p> <p>(d) Financing the offences established in accordance with subparagraphs (a) to (c) of this paragraph, which States Parties may establish as a separate offence.</p> <p>2. For the purposes of this article, the term “child sexual abuse or child sexual exploitation</p>	<p>imprisonment for a term of not more than 14 years and to a minimum punishment of imprisonment for a term of one year.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 163.1 (2)).</p> <p>Distribution, etc. of Child Pornography:</p> <p>Every person who transmits, makes available, distributes, sells, advertises, imports, exports or possesses for the purpose of transmission, making available, distribution, sale, advertising or exportation any child pornography is guilty of an indictable offence and liable to imprisonment for a term of not more than 14 years and to a minimum punishment of imprisonment for a term of one year.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 163.1 (3)).</p> <p>Definition of Child Pornography:</p> <p>In this section, child pornography means</p> <p>(a) a photographic, film, video or other visual representation, whether or not it was made by electronic or mechanical means,</p>
---	--

<p>material” shall include visual material, and may include written or audio content, that depicts, describes or represents any person under 18 years of age:</p> <p>(a) Engaging in real or simulated sexual activity;</p> <p>(b) In the presence of a person engaging in any sexual activity;</p> <p>(c) Whose sexual parts are displayed for primarily sexual purposes; or</p> <p>(d) Subjected to torture or cruel, inhumane or degrading treatment or punishment and such material is sexual in nature.</p> <p>3. A State Party may require that the material identified in paragraph 2 of this article be limited to material that:</p> <p>(a) Depicts, describes or represents an existing person; or</p> <p>(b) Visually depicts child sexual abuse or child sexual exploitation.</p> <p>4. In accordance with their domestic law and consistent with applicable international</p>	<p>(i) that shows a person who is or is depicted as being under the age of eighteen years and is engaged in or is depicted as engaged in explicit sexual activity, or</p> <p>(ii) the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region of a person under the age of eighteen years;</p> <p>(b) any written material, visual representation or audio recording that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act;</p> <p>(c) any written material whose dominant characteristic is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act; or</p> <p>(d) any audio recording that has as its dominant characteristic the description, presentation or representation, for a sexual purpose, of sexual activity with a person</p>
--	--

<p>obligations, States Parties may take steps to exclude the criminalization of:</p> <p>(a) Conduct by children for self-generated material depicting them; or</p> <p>(b) The consensual production, transmission, or possession of material described in paragraph 2 (a) to (c) of this article, where the underlying conduct depicted is legal as determined by domestic law, and where such material is maintained exclusively for the private and consensual use of the persons involved.</p> <p>5. Nothing in this Convention shall affect any international obligations which are more conducive to the realization of the rights of the child</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 14).</p>	<p>under the age of eighteen years that would be an offence under this Act</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 163.1 (3)).</p>
<p>Article 15: Solicitation or Grooming for the Purpose of Committing a Sexual Offence Against a Child</p>	<p>Luring a Child:</p> <p>Every person commits an offence who, by a means of telecommunication, communicates with</p>

<p>1 Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the act of intentionally communicating, soliciting, grooming, or making any arrangement through an information and communications technology system for the purpose of committing a sexual offence against a child, as defined in domestic law, including for the commission of any of the offences established in accordance with article 14 of this Convention.</p> <p>2. A State Party may require an act in furtherance of the conduct described in paragraph 1 of this article.</p> <p>3. A State Party may consider extending criminalization in accordance with paragraph 1 of this article in relation to a person believed to be a child.</p> <p>4. States Parties may take steps to exclude the criminalization of conduct as described in paragraph 1 of this article when committed by children.</p>	<p>(a) a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence with respect to that person under subsection 153(1), section 155, 163.1, 170, 171 or 279.011 or subsection 279.02(2), 279.03(2), 286.1(2), 286.2(2) or 286.3(2);</p> <p>(b) a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or</p> <p>(c) a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person.</p> <p><i>(Criminal Code, RSC 1985, c C-46. s 172.1 (1)).</i></p> <p>Making Sexually Explicit Material Available to Child:</p>
---	---

<p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 15).</p>	<p>Every person commits an offence who transmits, makes available, distributes or sells sexually explicit material to</p> <p>(a) a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence with respect to that person under subsection 153(1), section 155, 163.1, 170, 171 or 279.011 or subsection 279.02(2), 279.03(2), 286.1(2), 286.2(2) or 286.3(2);</p> <p>(b) a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or</p> <p>(c) a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 171.1 (1)).</p>
--	---

<p>Article 16: Non-Consensual Dissemination of Intimate Images</p> <p>1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the selling, distributing, transmitting, publishing or otherwise making available of an intimate image of a person by means of an information and communications technology system, without the consent of the person depicted in the image.</p> <p>2. For the purpose of paragraph 1 of this article, “intimate image” shall mean a visual recording of a person over the age of 18 years made by any means, including a photograph or video recording, that is sexual in nature, in which the person’s sexual parts are exposed or the person is engaged in sexual activity, which was private at the time of the recording, and in respect of</p>	<p>Publication, etc., of an Intimate Image Without Consent:</p> <p>Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct, is guilty</p> <p>(a) of an indictable offence and liable to imprisonment for a term of not more than five years; or</p> <p>(b) of an offence punishable on summary conviction.</p> <p>Definition of Intimate Image</p> <p>(2) In this section, intimate image means a visual recording of a person made by any means including a photographic, film or video recording,</p>

<p>which the person or persons depicted maintained a reasonable expectation of privacy at the time of the offence.</p> <p>3. A State Party may extend the definition of intimate images, as appropriate, to depictions of persons who are under the age of 18 years if they are of legal age to engage in sexual activity under domestic law and the image does not depict child abuse or exploitation.</p> <p>4. For the purposes of this article, a person who is under the age of 18 years and depicted in an intimate image cannot consent to the dissemination of an intimate image that constitutes child sexual abuse or child sexual exploitation material under article 14 of this Convention.</p> <p>5. A State Party may require the intent to cause harm before criminal liability attaches.</p> <p>States Parties may take other measures concerning matters related to this article, in accordance with their domestic law and consistent with applicable international obligations.</p>	<p>(a) in which the person is nude, is exposing his or her genital organs or anal region or her breasts or is engaged in explicit sexual activity;</p> <p>(b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy;</p> <p>and (c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed.</p> <p><i>(Criminal Code, RSC 1985, c C-46. s 162.1 (1), 162.1 (2)).</i></p>
--	--

(United Nations, <i>Draft United Nations convention against cybercrime</i> , (7 August 2024), vol. 24-14137 at art. 16).	
--	--

Primarily through optional clauses, the *Convention* can deviate significantly from Canadian law in governing sexual offences. For child exploitation material, Member States can limit restricted material to only that which represents an existing person or is a visual depiction under Article 12 (2)(a)(b). The definition of child pornography in Canada includes a person who is or is depicted as being under the age of eighteen years, whether the formatting is visual, written, or audio. Another discrepancy exists in Article 12 (4)(b). The clause allows Member States to exclude the criminalization of consensual child exploitation material if the content is limited to the private use for minors and only depicts real or simulated sexual activity and or the sexual organs of a minor primarily for sexual purposes. In Canada, children cannot consent to any form of child pornography because child pornography itself is not legal.

The option to require an act of furtherance in Article 15 (2) is likewise inconsistent with Canadian law; communicating with a minor through a telecommunications system in the facilitation of a crime is criminalized in Canada. Member States can opt in or out of criminal penalties if it was believed the child was not a minor. Although a similar stipulation exists in Canadian law, it requires an individual to make all reasonable efforts to ensure the age of the individual beforehand (*Criminal Code*, s 171.1 (4)). Article 15 (5) allows for Parties to navigate whether solicitation or grooming is illegal for children to do amongst themselves. Although Canada handles youth justice in a separate court system, the *Youth Criminal Justice Act* does

have provisions for criminalizing sexual offences by minors (*Youth Criminal Justice Act*, SC 2002, c. 1, ss 2(1), 42(2)(o), 200(1)(c-f)(q-s)).

The greatest dissimilarity between the illegal dissemination or publication of intimate images is the option to require an intent to cause harm in Article 16 (5). In Canada, lack of consent or recklessness to obtain consent is criminal in relation to making intimate images available. Furthermore, Member States can elect to define material as intimate images (rather than sexual exploitation material) if Article 16 (3) and Articles 14(3)(a)(b) or 14(4)(b) are used to decrease criminalization. This is incompatible with Canada’s definition of child pornography.

Criminal Involvement

UN Draft Convention Against Cybercrime	Canadian Law
<p>Serious Crime:</p> <p>shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 2).</p>	<p>Serious Offence:</p> <p>Means an indictable offence under this or any other Act of Parliament for which the maximum punishment is imprisonment for five years or more, or another offence that is prescribed by regulation.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. S 467.1 (1)).</p>
<p>Article 19: Participation and Attempt</p> <p>1. Each State Party shall adopt such legislative and other measures as may be necessary to establish as a criminal offence, in accordance</p>	<p>Attempts:</p> <p>Every one who, having an intent to commit an offence, does or omits to do anything for the purpose of carrying out the intention is</p>

<p>with its domestic law, when committed intentionally, the participation in any capacity, such as that of an accomplice, assistant or instigator, in an offence established in accordance with this Convention.</p> <p>2. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, any attempt to commit an offence established in accordance with this Convention.</p> <p>3. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, when committed intentionally, the preparation for an offence established in accordance with this Convention.</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 19).</p>	<p>guilty of an attempt to commit the offence whether or not it was possible under the circumstances to commit the offence.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 24 (1)).</p> <p>Parties to Offence:</p> <p>Every one is a party to an offence who</p> <p>(a) actually commits it;</p> <p>(b) does or omits to do anything for the purpose of aiding any person to commit it;</p> <p>or</p> <p>(c) abets any person in committing it.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 21 (1)).</p> <p>Person counselling offence</p> <p>Where a person counsels another person to be a party to an offence and that other person is afterwards a party to that offence, the person who counselled is a party to that offence, notwithstanding that the offence was committed in a way different from that which was counselled.</p>
---	--

	(<i>Criminal Code</i> , RSC 1985, c C-46. s 22 (1)).
<p>Article 17:</p> <p>Must be established as Criminal Offences:</p> <p>(a) (i) The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of that person's actions;</p> <p>(ii) The concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime;</p> <p>(b) Subject to the basic concepts of its legal system:</p> <p>(i) The acquisition, possession or use of property, knowing, at the time of receipt, that such property is the proceeds of crime;</p>	<p>Laundering Proceeds of Crime:</p> <p>Everyone commits an offence who uses, transfers the possession of, sends or delivers to any person or place, transports, transmits, alters, disposes of or otherwise deals with, in any manner and by any means, any property or any proceeds of any property with intent to conceal or convert that property or those proceeds, knowing or believing that, or being reckless as to whether, all or a part of that property or of those proceeds was obtained or derived directly or indirectly as a result of</p> <p>(a) the commission in Canada of a designated offence; or</p> <p>(b) an act or omission anywhere that, if it had occurred in Canada, would have constituted a designated offence.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 462.31 (1)).</p>

<p>(ii) Participation in, association with or conspiracy to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the offences established in accordance with this article.</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 17).</p>	<p>Conspiracy:</p> <p>Except where otherwise expressly provided by law, the following provisions apply in respect of conspiracy:</p> <p>(c) every one who conspires with any one to commit an indictable offence not provided for in paragraph (a) or</p> <p>(d) every one who conspires with any one to commit an offence punishable on summary conviction is guilty of an offence punishable on summary conviction.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 465 (1)).</p>
---	--

The UN's definition of serious crime includes punishments that are less one year to Canada's five-year or greater definition of serious offences. Participation in any capacity of an offence outlined by the draft *Convention* is prohibited, but offences related to attempt and preparation are optional (United Nations, *Draft United Nations convention against cybercrime*, (7 August 2024), vol. 24-14137 at art. 17). In Canada, it is criminal to attempt or become a party in the commission of an offence. The variation between the Convention's predicate offence and Canada's laundering proceeds of crime is subtle; Canadian law criminalizes recklessness. Conspiracy in both documents is synonymous, Canada just specifies degrees of seriousness.

Liability, Adjudication, and Sanctions

UN Draft Convention Against Cybercrime	Canadian Law
<p>Article 18: Liability of Legal Persons</p> <p>Each State Party shall adopt such measures as may be necessary, consistent with its legal principles, to establish the liability of legal persons for participation in the offences established in accordance with this Convention.</p> <p>2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative.</p> <p>3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences.</p> <p>4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.</p>	<p>Every one, Person and Owner, and Similar Expressions, include Her Majesty and an organization</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 2).</p> <p>Fundamental Principle:</p> <p>A sentence must be proportionate to the gravity of the offence and the degree of responsibility of the offender.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 718.1 (1)).</p> <p>Other Sentencing Principles:</p> <p>A court that imposes a sentence shall also take into consideration the following principles:</p> <p>(a) a sentence should be increased or reduced to account for any relevant aggravating or mitigating circumstances relating to the offence or the offender, and, without limiting the generality of the foregoing,</p>

<p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 18).</p>	<p>(i) evidence that the offence was motivated by bias, prejudice or hate based on race, national or ethnic origin, language, colour, religion, sex, age, mental or physical disability, sexual orientation, or gender identity or expression, or on any other similar factor,</p> <p>(ii) evidence that the offender, in committing the offence, abused the offender’s intimate partner or a member of the victim or the offender’s family,</p> <p>(ii.1) evidence that the offender, in committing the offence, abused a person under the age of eighteen years,</p> <p>(ii.2) evidence that the offender involved a person under the age of 18 years in the commission of the offence,</p> <p>(iii) evidence that the offender, in committing the offence, abused a position of trust or authority in relation to the victim,</p> <p>(iii.1) evidence that the offence had a significant impact on the victim, considering</p>
--	---

	<p>their age and other personal circumstances, including their health and financial situation,</p> <p>(iii.2) evidence that the offence was committed against a person who, in the performance of their duties and functions, was providing health services, including personal care services,</p> <p>(iv) evidence that the offence was committed for the benefit of, at the direction of or in association with a criminal organization,</p> <p>(v) evidence that the offence was a terrorism offence,</p> <p>(vi) evidence that the offence was committed while the offender was subject to a conditional sentence order made under section 742.1 or released on parole, statutory release or unescorted temporary absence under the Corrections and Conditional Release Act, and</p> <p>(vii) evidence that the commission of the offence had the effect of impeding another</p>
--	--

	<p>person from obtaining health services, including personal care services</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 718.2).</p>
<p>Article 21: Prosecution, Adjudication, and Sanctions</p> <p>1. Each State Party shall make the commission of an offence established in accordance with this Convention liable to effective, proportionate and dissuasive sanctions that take into account the gravity of the offence.</p> <p>2. Each State Party may adopt, in accordance with its domestic law, such legislative and other measures as may be necessary to establish aggravating circumstances in relation to the offences established in accordance with this Convention, including circumstances that affect critical information infrastructures.</p> <p>3. Each State Party shall endeavour to ensure that any discretionary legal powers under its domestic law relating to the prosecution of persons for offences established in accordance</p>	<p>Legal Rights to Apply to Those Charged with an Offence:</p> <p>Any person charged with an offence has the right:</p> <ul style="list-style-type: none"> a. to be informed without unreasonable delay of the specific offence; b. to be tried within a reasonable time; c. not to be compelled to be a witness in proceedings against that person in respect of the offence; d. to be presumed innocent until proven guilty according to law in a fair and public hearing by an independent and impartial tribunal; e. not to be denied reasonable bail without just cause; f. except in the case of an offence under military law tried before a military tribunal,

<p>with this Convention are exercised in order to maximize the effectiveness of law enforcement measures in respect of those offences and with due regard to the need to deter the commission of such offences.</p> <p>4. Each State Party shall ensure that any person prosecuted for offences established in accordance with this Convention enjoys all rights and guarantees in conformity with domestic law and consistent with the applicable international obligations of the State Party, including the right to a fair trial and the rights of the defence.</p> <p>5. In the case of offences established in accordance with this Convention, each State Party shall take appropriate measures, in accordance with its domestic law and with due regard to the rights of the defence, to seek to ensure that conditions imposed in connection with decisions on release pending trial or appeal take into consideration the need to ensure the presence of the defendant at subsequent criminal proceedings.</p>	<p>to the benefit of trial by jury where the maximum punishment for the offence is imprisonment for five years or a more severe punishment;</p> <p>g. has the right not to be found guilty on account of any act or omission unless, at the time of the act or omission, it constituted an offence under Canadian or international law or was criminal according to the general principles of law recognized by the community of nations;</p> <p>h. if finally acquitted of the offence, not to be tried for it again and, if finally found guilty and punished for the offence, not to be tried or punished for it again;</p> <p>i. if found guilty of the offence and if the punishment for the offence has been varied between the time of commission and the time of sentencing, to the benefit of the lesser punishment.</p> <p><i>Canadian Charter of Rights and Freedoms</i> [Charter], Part I of the <i>Constitution Act</i>,</p>
--	---

<p>6. Each State Party shall take into account the gravity of the offences concerned when considering the eventuality of early release or parole of persons convicted of such offences.</p> <p>7. States Parties shall ensure that appropriate measures are in place under domestic law to protect children who are accused of offences established in accordance with this Convention, consistent with the obligations under the Convention on the Rights of the Child and the applicable Protocols thereto, as well as other applicable international or regional instruments.</p> <p>8. Nothing contained in this Convention shall affect the principle that the description of the offences established in accordance with this Convention and of the applicable legal defences or other legal principles controlling the lawfulness of conduct is reserved to the domestic law of a State Party and that such offences shall be prosecuted and punished in accordance with that law.</p>	<p>1982, being Schedule B to the <i>Canada Act</i> 1982 (UK), 1982, c 11. s 11 (1)).</p> <p>Shall be Deemed to be Aggravating Circumstances:</p> <p>(b) a sentence should be similar to sentences imposed on similar offenders for similar offences committed in similar circumstances;</p> <p>(c) where consecutive sentences are imposed, the combined sentence should not be unduly long or harsh;</p> <p>(d) an offender should not be deprived of liberty, if less restrictive sanctions may be appropriate in the circumstances; and</p> <p>(e) all available sanctions, other than imprisonment, that are reasonable in the circumstances and consistent with the harm done to victims or to the community should be considered for all offenders, with particular attention to the circumstances of Aboriginal offenders.</p> <p>(<i>Criminal Code</i>, RSC 1985, c C-46. s 718.2).</p>
---	--

<p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 21).</p>	
<p>Article 20: Statute of Limitations</p> <p>Each State Party shall, where appropriate, considering the gravity of the crime, establish under its domestic law a long statute of limitations period in which to commence proceedings for any offence established in accordance with this Convention and establish a longer statute of limitations period or provide for the suspension of the statute of limitations where the alleged offender has evaded the administration of justice.</p> <p>(United Nations, <i>Draft United Nations convention against cybercrime</i>, (7 August 2024), vol. 24-14137 at art. 20).</p>	<p>Summary Convictions (Limitation):</p> <p>No proceedings shall be instituted more than 12 months after the time when the subject matter of the proceedings arose, unless the prosecutor and the defendant so agree (<i>Criminal Code</i>, RSC 1985, c C-46. s 786 (2)).</p> <p>Unless otherwise provided by law, every person who is convicted of an offence punishable on summary conviction is liable to a fine of not more than \$5,000 or to a term of imprisonment of not more than two years less a day, or to both. (<i>Criminal Code</i>, RSC 1985, c C-46. s 787 (1)).</p> <p>Indictable offences: more serious and include theft over \$5,000, break and enter, aggravated sexual assault and murder. Maximum penalties vary and include life in</p>

	prison. Some have minimum penalties. There is no statute of limitations on indictable offences. (Government of Canada, 2021a).
--	---

Member States are at liberty to recognize aggravating circumstances; Canada has many for criminal offences. Clauses requiring justice be consistent with human rights standards are evidently consistent with Canadian law. Statutes of limitations are largely open to domestic interpretation under Article 20. In Canada, summary convictions that carry a fine or two years less a day in imprisonment are subject to a twelve month statute of limitations. There is no statute of limitations for indictable offences.

Civil and administrative jurisdictions extend beyond the scope of this research and are therefore not paired to an alternative in Canadian law.