2022

Fifth-Dimensional Warfare and National Security in Canada: Situating Microdeviation Theory Within C-59: An Act Respecting National Security Matters

Hayden Slight
slig8390@mylaurier.ca

Fifth-Dimensional Warfare and National Security in Canada:

Situating Microdeviation Theory Within C-59: An Act Respecting National Security Matters

by

Hayden Slight

Master of Arts, Wilfrid Laurier University, 2022

THESIS

Submitted to the Department/Faculty of Criminology

in partial fulfilment of the requirements for

Master of Arts in Criminology

Wilfrid Laurier University

ABSTRACT

In an era of rapid technological change, the growing threat environment in the cyber dimension will continue to influence how a sovereign nation contends with attacks that can occur from any corner of the world. The growing adaptation and expansion of technology belonging to the Internet of Things (IoT) and the increasing prevalence of social media (Facebook, Twitter) has also influenced the spreading of attack surfaces that can become victim to exploitation by motivated parties including foreign states and terrorist groups. Against this backdrop, Canada's own efforts to modernize and reinforce its own national security agencies resulted in the developing and royal assent of 2017's Bill C-59: *An Act Respecting National Security Matters*. The royal assent of C-59 poses a unique opportunity to examine the underlying narratives and evidence used by expert witnesses and committee members alike to frame the threat that the cyber environment has when influencing C-59's more controversial measures. This includes the expansion of the Communication Security Establishment's (CSE) traditional 3-part mandate to include the use of cyberoperations, or the expansion of Canada's nation security agencies to utilize the loosely defined "public datasets" despite concerns of possible misappropriation. Utilizing Popham's (2018) Theory of Microdeviation, this thesis highlights the normalized experiences of Canadians online when considering the exploitation of IoT technology and social media to conduct attacks or sabotage against democratic states, and how these narratives were often used to advance C59's modernization push. Finally, this thesis also analyzes the implications of C-59 when considering the international community as it relates to a growing cyber arms race akin to 20th century Cold War fears, and how Microdeviation Theory has utility when examining the goals of legislation seeking to control deviant behaviour online.

ACKNOWLEDGEMENTS

In an effort to contain my own appreciations to a single page, I'd like to first and foremost thank my Dad for his years of unending support on a whim 10 years ago when I made the drastic career change to policing that would culminate in a Master's Degree of all things. Your help through many of my hardships along the way is a debt I'll likely never be able to repay but will hopefully come close.

Next, I would like to thank my better half, Emma, for her unending love and support through everything a pursuit of higher education has, including the extreme lows. Despite coming into my life halfway through this, anyone else would have likely left by now and I'll likely spend the rest of my life hoping to gain a glimpse of why you didn't. I love you, despite your best advice to my thesis' objectives being the quite possibly true words "just log off".

Including everyone in the Department of Criminology, I'd also like to extend my thanks to Dr. James Popham, for all his advice and instruction over the years including my undergraduate. You're the professor who set this whole M.A. career off, and luck would have it that I would take hold of your theory and see it as a new way to examining criminological theory in all things digital.

I'd also like to thank Dr. Patrick Watson, who afforded me so much in my graduate career, including a trip to Hong Kong to discuss possible PhD work and presenting our research to Facebook which gave me my first glimpse into the professional world of research that I hope to keep going.

Lastly, this thesis is dedicated to Luna Slight, the rock throughout this whole pandemic mess who left this world way before her time. You were there to greet me in the morning, and the last thing I'd see whenever stress kept me up at night as you gave me more affection than I ever deserved. I miss you more than words can say and hope you're having the time of your life across that rainbow bridge that you never got to have here.

LIST OF ABBREVIATIONS

Canadian Security Intelligence Service	…CSIS
Communications Security Establishment	…CSE
Critical Appraisal Skills Programme	…CASP
European Union	…EU
Intelligence Commissioner	…IC
Internet Corporation for Assigned Names and Numbers	…ICANN
International Humanitarian Law	…IHL
Internet of Things (also SMART Technology)	…IoT
International Telecommunications Union	…ITU
Internet Research Agency	…IRA
National Intelligence Review Agency	…NSIRA
North Atlantic Treaty Organization	…NATO
Royal Canadian Mounted Police	…RCMP
Security and Intelligence Threats to Elections	…SITE

TABLE OF CONTENTS

INTRODUCTION

Against the backdrop of unfettered and rapid technological advancement in a digital age, the boundaries that delineate theatres of war or where the physical embodiments of a person end and the digitalized self begin are continuing to erode. The benefits that digital technologies in particular have provided an increasingly crucial component to the function of every Canadians livelihood as more devices become integrated into the Internet of Things (IoT). Advancements made into the proficiency of internet technology such as the advent of social media platforms or the proliferation of SMART technology (i.e., the integration of traditional products such as appliances to the internet with advanced features) has enabled luxuries to the social lives of individuals by providing near instantaneous connections to global communities and resources. For the purpose of this paper, Maras (2015) defines the IoT as it “refers to the connection of everyday objects (eg TVs, appliances, and exercise equipment) to the Internet. It enables the real-time monitoring and vast collection of data about property, people, plants, and animals” (pg. 99). However, this proliferation and subsequent integration of the internet and social media has also posed additional problems when considering the overt dependence on the platform as an avenue of information that can be tailored or filtered to an individual’s preferences (Arayankalam & Krishnan, 2021; Bradshaw & Howard, 2018). In recent years, this dependence by users internationally has become subject to misinformation campaigns via foreign states and terrorist groups that seek to proliferate divisive or radicalized content that can have adverse impacts outside of the platform and threaten national security by forgoing traditional weaponry in favor or creating vice amongst populations or leveraging contemporary technology as acts of aggression (Arayankalam & Krishnan, 2021). Following the revelations of disinformation campaigns being utilized in the 2016 United States Presidential Election, Canada’s own national security agencies, the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS) had published several reports warning of the threat that rapidly evolving technology and misinformation campaigns can inflict upon Canada (CSE, 2018; CSIS, 2018). A notable factor to these concerns is that Canadian usage of IoT technology and growing utilization of social media platforms has itself presented a potential threat to Canada's national security as these platforms are exploited for varying degrees of malicious gain.

Being a relatively new development, the advent of social media and rapid onset of digitally extending the social lives of individuals poses significant questions to whether certain consumption behaviours online can be effectively legislated or protected from exploitation. While social media platforms have provided a new form of digitally connecting with other like-minded individuals, it has also opened the door for criminally motivated bodies to exploit the underlying function of these platforms and utilize them in such a way to further sow discord and extremism that translates into real-world events (Bradshaw & Howard, 2018). A notable example of this strategy concerns the utilization of disinformation on social media platforms against Ukraine citizens by Russia to advance pro-Russia separatism, prevent Ukraine's transformation into part of the external border of NATO and the EU, and alleviate global sanctions brought forth from Russia's initial invasion of Crimea (Forrester, Bacovcin, Devereaux, & Bedoya, 2019). Further complicating this concerns prior attempts at legislating online behaviours and their inability to effectively regulate behaviours online while adhering to Charter protection (Taylor, 2016).

CSIS' *Disinformation Report*, which saw the convergence of scholars and professionals to discuss and highlight new and growing threat environments to Canada, specifically noted foreign interference threats that Russia and China posed regarding the growing use of social media platforms and internet technology as a part of their own national security strategies to advance foreign policy objectives (2018). This included the hijacking of traditional social media platforms to further spread disinformation favorable to the state's foreign policy objectives and weaken the cognitive resistance of a states populace to greatly enable the spread of false news or narratives online (Buchanan, 2020). CSIS' (2018) report also highlighted how these platforms are being utilized by motivated individuals and groups across different ideological and political spectrums to advance radical narratives as factual and drive recruitment of vulnerable individuals. Once a narrative or perspective is established, they will use social media or digital news outlets to ensure posts go viral ensuring its acceptance among other users (page 17). As an example, the report highlights a 2017 mass shooting in Texas where a 26-year-old was identified who had a history of domestic violence and was discharged from the US Air Force as being the suspect. The report further notes that "however, before that narrative developed, and then continuing even after it had been established, an alternative narrative claimed that the suspect was really an Antifa terrorist" (p.16) and had already begun to weaponize doctored media and exploit social media platforms to perpetuate the disinformation on the suspect. The report additionally noted the organizations that host these platforms have been reluctant to addressing the issue of moderating disinformation, either by willful ignorance or interestingly a position that these platforms need to maintain a philosophical position to the open sharing of information (page 10). A critical point to be taken from both CSIS and CSE reports on modern national security threats is that IoT advancements in both social media and the internet in the context of an increasing reliance by Canadians is continuing to open new paths to exploitation by both foreign and domestic threats.

The threat that these internet products pose towards democratic institutions and critical infrastructure were some of the key drivers in securing the royal assent of 2017s *Bill C-59: An Act Respecting National Security Matters*. Introduced by the then Liberal majority government, the legislation sought to modernize Canada's national security strategies against the backdrop of an evolving threat landscape while also rectifying controversial measures contained in its predecessor, *Bill C-51: Anti-Terror Act (2015)*. A radical piece of legislation, the bill brought sweeping reform to the overall structure, oversight, and mandates of Canada's national security agencies, namely, the Communications Security Establishment (CSE) and the Canadian Security Intelligence Service (CSIS) (West, 2018). This act received royal assent and thus came into force in June 2019. C-59 also addressed oversight and review shortcomings of its predecessor C-51 by merging the agencies respective review committees (Notably, the Security Intelligence Review Committee and the CSE Commissioner) and formalizing the Intelligence Commissioner (IO) office for the purposes of authorizing and reviewing the activities carried out by the respective agencies (Nesbitt & West, 2019). As Canada's primary signals intelligence agency, the CSE is tasked with protecting critical Federal electronic infrastructure and communication networks, providing foreign intelligence as it relates to Canadian national security, and is the primary authority for cyber security and information assurance (Parsons, Gill, Israel, Robinson, & Deibert, 2017). Under the guise of requiring a modernized national security strategy and a revisit towards C-51's controversial amendments, C-59 represents the first time in Canadian history that the CSE be established under its own legislative constitution, while also empowering the agency with 2 new directives under its then 3-part mandate that dramatically empowers the agency with new cyber-capabilities to assist in carrying out their objectives (West, 2018). Prior to C-59, CSE' mandates were contained in the *National Defence Act* (NDA). Section 273.64(1) of the NDA outlined the agencies mandates as “a” “b”, and “c” whereby:

a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties

While C-59 brought these mandates under sections 16, 17, and 18 of the *Communications Security Establishment Act*, sections 19 and 20 in C-59 provides the legislative authority to expanding CSE’ mandate to utilize new measures to become a more active role in Canada’s national security strategies through cyberoperations:

19) The defensive cyber operations aspect of the Establishment’s mandate is to carry out activities on or through the global information infrastructure to help protect
    a. federal institutions’ electronic information and information infrastructures; and
    b. electronic information and information infrastructures designated under subsection 22(1) as being of importance to the Government of Canada.

20) The active cyber operations aspect of the Establishment’s mandate is to carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign

> individual, state, organization or terrorist group as they relate to international affairs, defence or security.

In relation to the digital capabilities of Canada's own national security agencies, these new powers have been subject to criticism from academia, political, and civil rights groups in Canada given the already unknown nature of CSE activities prior to C-59's enactment (Nesbitt & West, 2019; West, 2018). Furthermore, C-59 empowers CSE with the capacity to employ cyberoperations that include disruption, sabotage, interference, and influence towards foreign individuals, states, organizations, and terrorist groups as countermeasures against presumed threats. These mandates have drawn heavy concern towards the future of warfare and explicit condoning of state-sponsored hacking (West, 2018). Whereas it is becoming more important to understand the rapidly changing threat environment that both foreign and domestic bodies have on Canada's national security, this digital arms race harkens back to the Cold War and the threat that it has on unknowingly implicating Canadians in acts of war.

i. Microdeviations and Research Statement

Given the radical new powers granted to Canadian intelligence agencies through C-59, the main aspect of this thesis is to propose assessing committee meetings and expert witness supplemental briefs regarding C-59 through the recently developed Theory of Microdeviation (Popham, 2018) and to provide an analysis on the relationship that the evolution of IoT technology and the internet has alongside their growing integration amongst users against traditionalist criminological perspectives that incorporates a technosocial perspective as examined by Brown (2006) who devises the Criminology of Hybrids as thus:

> Suppose criminology looked outside both the modern 'nature-culture' divide *and* the late modern deconstructionist projects, *and* beyond the governmentalists' highly social

> notions of technology, towards theories of the technosocial: the cyber, the data human, the cybernetic and even the a-modern. What sort of contributions, what challenges, might such theorizations make to analyses of crime, law and control? (p.711)

As such, this thesis will consider itself towards 3 objectives: How do expert witnesses and government officials presenting to the House of Commons and Senate committees employ narratives and evidence relative to manufactured uncertainty and national security threats online to justify some of the possible disproportionate measures contained in Bill C-59? Second, given the prevailing narratives towards modernization and futureproofing that informed C-59 and the failures of provincial government attempts at controlling cyber-deviant behaviour online, does the integration of Browns (2006) *Criminology of Hybrids* perspective have merit in explaining how technosocial perspectives account for the melding of human and technology? The final question will seek to ask; can the integration of Microdeviation Theory provide context on how legislation informed by manufactured uncertainty may unknowingly breach Charter rights? As described by Popham (2018), microdeviations entails the generation of manufactured uncertainty about the internet and technology to facilitate the passing of legislation that is disproportionate and overtly punishing towards implicated targets. This will include examining testimony made by both expert witnesses and committee members focusing on the multitude of aspects concerning the growing threat landscape online, Canadians general understanding of data privacy and cyberthreats online, and testimony that considers the possibility of disproportionate implications that these new powers in C-59 may have.

This application of Microdeviation Theory as it pertains to C-59 will allow the examination of expert witness testimony that incorporates the normalization of digital threat environments and the utilization of manufactured uncertainty towards the evolution of the internet and technology to justify legislation that can be disproportionate outside of what they were meant to control. One such example can be seen in CSE's (2019) report about foreign interference towards Canada, notably how this primarily occurs through the dissemination of materials through social media networks like Facebook and Twitter by use of bots and "troll farms" to target voters and sway political behaviour in favor of disrupting democratic processes. Whereas Popham (2018) introduced microdeviations into political discourse through actions such as astroturfing campaigns to sway public opinion, this thesis will expand and test this theory to account for how manufactured uncertainties about cyberspace can influence actors at the federal level in proposing and rationalizing why certain aspects of C-59 are needed to better modernize Canada's national security agencies. As such, a defining aspect of this research entails a unique perspective of examining the complexities of cybercrime taxonomy while also advancing theoretical discussions on criminology's larger role in examining the relationship between technology and crime. As will be discussed in the forthcoming review of academic literature, the main body of research surrounding C-59 and both IoT and social media ecosystems generally will focus on the key implications to international relations (the law of self-defence) and user-based susceptibility to foreign disinformation campaigns that circulate online via social media. Furthermore, this review will also highlight how C-59's path to royal assent presents a gap in scholarly research concerning the application of technosocial perspectives and Microdeviation Theory when considering how Federal legislation situates Canada's current threat environment.

Given the complex nature of this thesis, qualitative sources in information pertaining to C-59 will be limited to the committee minutes and supplemental briefs that were submitted during key debate sessions held to discuss how C-59 would proceed by having expert witnesses testify on matters pertaining to the bill's development. These sources are readily archived and obtainable through the Canadian Federal Governments website which will facilitate a non-obtrusive approach to examining the proposed research objectives contained here (https://www.ourcommons.ca/Committees/en/SECU/StudyActivity?studyActivityId=9807256#DT20171130SECUMEE88ID9807256). By focusing on these documents, it will be feasible to examine pivotal moments in the leadup to C-59's royal assent. And will highlight the intricacies of the nature of modern digital threat landscapes and drafting effective legislation based on the perspectives of leading experts in digital infrastructure.

RESEARCH BACKGROUND

i. Introduction

This section of the thesis seeks to situate the perspectives that will be taken when examining C-59. This background section will aim to provide relative context to the reader by presenting sources that deal with difficulties that Canadian governments both federally and provincially have encountered when implementing legislation concerning online behaviours. Furthermore, scholarly critiques of the bill will be presented to demonstrate the primary concerns of certain sections including government oversight and disproportionate consequences. Lastly, this section will include scholarly sources that examine how digital media sources are often subject to malicious attempts of distortion, divisiveness, and utilization of political extremist groups to promote narratives and influence individuals online to promote anti social-justice agendas.

ii. Canadian Legislative Responses

One of the most recent examples of cybercrime legislation concerns the repealing of Nova Scotia's provincial *Cyber Safety Act*. At issue here that to draft effective and constitutional legislation regarding cyberbullying, its inherent definition must leave no room for multiple interpretations as it can pose significant threats to Charter rights granted to citizens (Taylor, 2016). The core purpose of the *Cyber Safety Act* attempted to give a legislative definition to cyberbullying, articulate when cyberbullying becomes an actionable offence, as well as provide legislative remedies that victims could pursue against the accused. Taylor's work in the subject focused on the discussion from Justice McDougall's 2015 ruling in *Crouch v. Snell*, which tested the *Cyber Safety Act's* constitutionality focusing on the bill's overtly vague description of online behaviours and its use of excessive penalties that far outstretched constitutional protections as per the *Oakes* test. For clarity, the *Oakes* test sets out whether a Federal or Provincial legislation can withstand a section 1 challenge from the Canadian Charter. Section 1 of the Canadian charter concerns itself with two scenarios; that the challenged legislation is objectively clear, and should the legislation violate any Canadian Charter right, that the violation is as minimal as possible. This is further highlighted when we consider the shift of how people interact with each-other politically: a contemporary example concerns the recent Quebec City Mosque attack perpetuated by Alexandre Bissonnette, who throughout his subsequent trial was found to have been obsessively consuming large quantities of right-wing media online prior to committing the shooting. Some of the content included material on President Donald Trump's controversial travel ban towards Muslims and Middle Eastern countries, and conspiracy theory/white supremacist outlets that would often publish content depicting the apparent imposition of Sharia Law on western nations (Riga, 2018). Like *Crouch v. Snell* in legislating cyberbullying effectively, the case of Bissonnette has the potential to inquire about whether it's possible within constitutional grounds to legislate consumption behaviours online for the purposes of national security and still withstand Charter challenges.

In their 2019 cyber threat report, CSE noted that Canada is very likely be targeted by foreign nations through disruption campaigns that would seek to influence Canadian voters of the then upcoming 2019 federal election through different facets of internet culture such as social media feeds, forums, and published media content (p. 5). Although the implication of these disinformation campaigns was anticipated to have a smaller affect compared to the 2016 U.S. election misinformation campaign, CSE also noted that since their previous report in 2017 that "political parties, candidates, and their staff have continued to be targeted worldwide by cyber threat activity - though to a lesser extent than voters" (p. 5). Internationally, the report notes that of all cyber threat activity online, that approximately 88% of incidents recorded had been strategically motivated, defined by the report that "threat actors specifically targeted a national democratic process for the purpose of affecting the outcome" (p. 15).

The lead up to and post results of the 2019 Canadian Federal Election saw a variety of crucial policies and subsequent reports that highlighted the need to be vigilant and adaptive to the radically changing nature of the internet. This included the formation of the Security and Intelligence Threats to Elections (SITE) task force to monitor and alert the public to significant cyber threats against the election (Cain, 2019), the final drafting and royal assent of Bill C-59: *An Act Respecting National Security Matters* (West, 2018) which included aforementioned measures relating to cyber defence and formally established the mandate of the CSE, and the subsequent reports that emerged post election that illustrated the various attempts at manipulation campaigns towards Canadian voters. This included a report by Nexology that examined computer bot behaviours in producing content targeting anxieties regarding immigration and refugee status, the Canadian economy, as well as producing reactionary content to generate inclusion of extremist ideologies across both sides of the political spectrum (Forrester, Bacovcin, Devereaux, & Bedoya, 2019). Utilizing blacklists such as www.propornot.com, a website that identifies sites that produce or propagate Russian propaganda, one such finding identified bot accounts that "were pushing a largely leftward (politically) leaning set of themes e.g. destroying organic farms or pro-Iranian and anti-Saudi messages" (p. 7). The report further notes that whereas the 2016 U.S. Presidential Election saw foreign agencies based in Russia utilize disinformation campaigns and social media manipulation online in favor of then Presidential candidate Donald Trump, tactics used during the 2019 Canadian federal election instead sought to create voter disenfranchisement by propagating narratives online to create contestation between Canadian users and further generate apathy towards democratic institutions.

iii. Scholarly Responses to Bill C-59

The threats that foreign state adversaries have and their capabilities towards leveraging digital avenues such as the internet or the development of technological weaponry was a key driver behind some of the more controversial aspects of C-59 when it was first introduced in 2017. The bill was met with controversy among legal scholars concerning the expansion of powers granted to CSIS and CSE as it relates to online surveillance and signals intelligence sharing with both domestic and international intelligence agreements (Nesbitt & West, 2019; Parsons, Gill, Israel, Robinson, & Deibert, 2017; Nesbitt, 2020). Regarding the expansion of powers granted to CSE, the leading concern among scholars focuses on the integration of the new *active* and *defensive* cyber operations that allow the agency to facilitate what has been regarded as an enabling of “state-sponsored hacking” against global IT infrastructure and foreign bodies (Parsons, Gill, Israel, Robinson, & Deibert, 2017; West, 2018). Essentially, these operations can include generating malware attacks against critical IPS infrastructure globally to disrupt foreign aggressors as well as gathering massive amounts of data that is publicly available or can be purchased via the commercial market, which carries with it the possibility of innocent Canadians abroad being affected despite mandates specifically barring the agency from doing so. Additionally, C-59 extends new powers to CSIS that effectively enable the agency to adopt a more proactive approach in conducting sabotage campaigns against suspected individuals. Concerns from scholars here focus on how CSIS can now (among other things) impersonate others, plant evidence, and apply to limit certain Charter rights of individuals involved in investigations should the newly established Intelligence Commissioner Office (IO) approve the application (West & Forcese, 2019).

Bill C-59 also implements new review measures by establishing the National Security and Intelligence Review Agency (NSIRA) and giving it the power to oversee all mandates of Canada’s intelligence agencies including CSIS, CSE, and the RCMP. However, this also resulted in the closing of all potential avenues for public review. C-59 serves as a replacement to the previous national security act, C-51, which at the time was mired in controversy to anti-terrorism measures such as the isolating of each agencies review bodies from collaboration when their respective agencies engaged in collaborative investigations (Roach & Forcese, 2015). In their critique of C-51, Roach and Forcese (2015) note that previous review bodies were only capable of reviewing the conduct of their respective agency and were unable to conduct joint investigations such as when the RCMP would work with CSIS on potential domestic terrorism cases. This resulted in gaps between annual reviews since the collaborative nature between agencies would stifle inquiries when parts of investigations were handed off to another agency. While the addition of the NSIRA was a key benefit, the coupling of these new (and vaguely defined) powers against the backdrop of public internet privacy and a growing digital threat landscape have influenced why these concerns are so prevalent with C-59’s wording.

iv. Disinformation and Sabotage in a Digital Era

The implementation of C-59 poses a unique opportunity to examine how governmental perceptions of the growing number of internet-borne threats have begun to shift in response to recent encroachments into Canadian digital infrastructures, such as the growing global awareness about disinformation campaigns (Marwick & Lewis, 2017). Furthermore, the status of C-59 and its royal assent put fourth questions about how the use of seemingly benign internet platforms such as Facebook and Twitter were utilized in the 2016 U.S. presidential race by Russia to target and disrupt critical voter states to secure the election of Donald J. Trump (McCombie, Uhlmann, & Morrison, 2019). In other words, a key revelation notes how the increasing perversion of social media, other internet platforms, or devices being connected online as an avenue to all facets of information for an individual can expose them to misinformation campaigns online while also expanding avenues to threats online as critical infrastructures become increasingly dependent on the internet for connectivity.

Whereas C-51 has been regarded as being a political response towards the two terrorist attacks that saw the death of two CAF members on Parliament Hill and the Saint-Jean sur-Richelieu terrorist ramming (Nesbitt, 2020; Roach & Forcese, 2015), C-59 was touted by government representatives as modernizing Canada’s national security agencies via the expansion of digital powers to their mandates to be better equipped against internet-borne attacks from threats both foreign and domestic. It is important to note here however, that the proposed research itself is not concerned with providing a critical analysis of whether the new and expanded powers contained in C-59 are warranted. Rather, this thesis will assess how the utilization of extreme cases of internet and social media manipulation alongside contemporary threat environments and the rapidly evolving digitalized societies has influenced the reactionary nature of Bill C-59.

LITERATURE REVIEW

i. *Introduction*

The following chapter aims to integrate a sufficient catalogue of the prevailing scholarly work related to the multitude of subject matter considering both cyber-deviant behaviours and Canada’s own national security strategies. This includes prior scholarly work that considers the role that social media and IoT technology have when used to conduct attacks both foreign and domestically against national security interests. Further, this chapter will also provide an account of existing research that considers differing forms of governance towards multiple aspects of online cultures and contemporary technology. This includes attempts made by provincial governments towards controlling the impacts of cyberbullying and C-59’s predecessor C-51 that saw the expansion of powers granted to Canada’s NSAs when considering the collection and exploitation of digitalized datasets for the purpose of maintaining security. To conclude, this chapter will examine existing literature that focuses on Canada’s Supreme Court interpretations to the protection of privacy online as well as existing scholarly work surrounding digital privacy in a rapidly evolving society.

ii. Digital Content Manipulation and Sabotage Online

As popular social media applications such as Facebook and Twitter continue to dominate the global market as a primary source of information and livelihood for its majority of users, the threats posed by disinformation campaigns and content manipulation online will continue to be an issue that will become more difficult to control. Scholarly efforts typically examine the uptick in users accessing social media platforms or forum-based webpages and how users increasingly interact with one another digitally (Massanari, 2017; Marwick & Lewis, 2017). One example concerns how Twitter can become a hosting ground to manipulation or conflict between users that can often draw serious implications outside of the platform. This has included recent events such as the #gamergate incident that saw a countercultural revolt against a perceived lack of ethics in video game journalism culminate in attacks on feminism activists as well as minority game developers, reporters, and reviewers alike (Massanari, 2017; Nagle, 2017). Additionally, recent developments surrounding social media's involvement in disinformation campaigns to sabotage the 2019 Canadian Federal Elections were also examined, which found that foreign interference campaigns were being conducted through bot campaigns that sought to aggravate wedge issues discussed online to allow foreign actors to operate with less resistance in their objectives (Forrester, Bacovcin, Devereaux, & Bedoya, 2019). Among others, these examples are illustrative of the rise in digital movements online reflective of political groups across the broader ideological spectrum or reactionary movements that classified as forms of "culture" or "flame" wars online (Nagle, 2017).

Regarding disinformation campaigns carried out by right-leaning groups, these conflicts have almost exclusively played out online, with the tactics that right-leaning and other reactionary groups use involving "hacks" that capitalize on the interactive design of social media users to recruit likeminded individuals on issues including social justice and racism (Lewis, 2018). Lewis defines such movements as being part of "alternative influence networks" whereby users will typically be drawn into extreme-leaning political online subcultures by framing social justice activities as direct attacks against the individual's culture and identity. Lewis (2018) further elaborates on how this digital network can effectively serve as a gateway to narratives of extreme racism and right-wing ideology by linking or networking multiple social media formats together along similar concepts. Actors in this network include notable white supremacist Richard Spencer, YouTube/Podcast host David Crowder, and conservative pundit Ben Shapiro among others (Nagle, 2017). To distance their own platforms from traditional media outlets, actors within this network will attempt to convey a unique sense of authenticity that distance themselves from “mainstream media outlets”. By engaging in these types of activities, Lewis (2018) notes that this allows for the actor to impart content towards their audiences that attempt to persuade them of popular right-wing narratives such as racial inequality towards Caucasians, vehemently oppose feminism, as well as “standing up” against social policies perpetuated by social justice warriors or in worse cases, people of the Jewish faith. However, these users do not typically pursue these agendas through normative means. Rather, users will often engage in banal behaviours such as posting tweets or generating forum posts that espouse their antagonistic beliefs against movements perceived as being progressive. Groups noted by Lewis and Marwick (2017) to also engage in online disinformation campaigns have included men’s rights activists, conspiracy theorists such as Alex Jones, and users of the popular forum page 4chan. This is partly in fact that while they may align on certain issues such as being against perceived progressive policies, these groups have been vehemently opposed to ideological narratives others may have such as white nationalism or anti-Semitism (Marwick & Lewis, 2017). Regardless, actors involved in far-right talking points or foreign interference will typically produce or manipulate content that serves their own (or combined) objectives to “game” social media algorithms and search engines alike that will allow the communication of these narratives to internet users (Marwick & Lewis, 2017; Nagle, 2017). By manipulating social media and search engine algorithms, actors in this network can artificially inflate the popularity of certain keywords or devise “viral” hashtag movements that allow for the content to appear prominently on other users’ feeds. An example of this comes from the #gamergate incident whereby far-right actors utilized the hashtag to drive discussion and harassment online. By driving the popularity of this hashtag, Marwick and Lewis (2017) articulate how it became a digital unifying keyword relative to organizing online campaigns. Considering these movements however, traditional media outlets fail to provide coverage to these campaigns as companies struggle to adapt to the changing media monetization online. Whereas extremist groups online have flourished, media companies often struggle to gain a foothold into the online market due to economic factors including a lack of trust among consumers and loss of advertising revenue to other free access sites such as Craigslist (Lewis, 2017). As such, smaller media outlets will often fold or be absorbed into larger media families that would rather focus on generating relatable content to a casual audience at the cost of providing more grounded and accurate coverage to viewers.

While the use of internet bots or campaigns to game trending algorithms is used by both right leaning and foreign government actors, this is not the only way to propagate specific agendas online. The utilization of digital new outlets, meme culture, and content specific forums are also used in tandem to manipulate media sources online (Marwick & Lewis, 2017; Forrester, Bacovcin, Devereaux, & Bedoya, 2019). Marwick & Lewis (2017) examined how far-right actors may engage in content manipulation to influence forms of 'agenda setting', whereby the goal of having manipulated content be covered does not concern the fact of whether the story is eventually debunked, but to simply have the content reported on and gain exposure in the first place. This has usually been achieved by having content driven "up the chain" of prominent news sources by initially planting a manipulated story in a smaller media outlet with lax fact checking procedures, in hopes that larger outlets will subsequently pick up the story (p. 38). An example of driving fake content to national coverage includes the case of "White Student Union" Facebook pages that were fabricated by white nationalist outlet The Daily Stormer founder Andrew Anglin with the hopes of having the groups covered nationally thereby potentially having university students join their movement (Marwick & Lewis, 2017). This technique is not limited to fake content, and far-right actors have also driven narratives on factual content by specifically framing the story in certain ways to promote their agendas. Marwick & Lewis (2017) note that when presented with evidence contradictory to their own beliefs, far-right actors will typically “double-down” on their own beliefs and set out to push a false narrative to their groups or audience to demonstrate their authenticity to others. Furthermore, the prevalence of meme culture and specific content forums such as 4chan have also been utilized with other disinformation techniques in publishing far-right narratives. The accessibility of meme culture can facilitate the least resistance in fabricating a viral campaign as they are concise in their objective and can be easily shared among others within or outside the group (Marwick & Lewis, 2017). Forums such as those found on The Daily Stormer and 4chan have often hosted specific days whereby users are encouraged to develop memes that can then be shared by other users on their own social media pages thus generating visibility on trending topics. Relative to microdeviation, digital content manipulation highlights not only the difficulties that media companies face to provide accurate and effective coverage, but also with how social media platforms and underlying services including content algorithms are subjected to hacks outside of their anticipated use.

Compared to political groups online, actors involved in foreign interference campaigns deviate slightly in their goals insofar as groups have been found to engage in reactionary politics online, but with the underlying purpose of distracting authentic users from other pertinent issues while also advancing acceptance towards the nation states foreign policy goals such as underscoring a populations belief in the integrity of democratic institutions (Bradshaw & Howard, 2018; Forrester, Bacovcin, Devereaux, & Bedoya, 2019). Concerning the broader international goals of these foreign campaigns, Bradshaw and Howard (2018) note that foreign adversaries will also hijack traditional social media technologies to employ the use of "soft power and persuasion, framing and agenda setting, ideological hegemony, symbolic power, or sharp power to achieve desired outcomes" (p.25). Drawing from the Computational Propaganda Project in 2017, they also note that depending on the type of regime (Democracy, Authoritarian, or Crisis State), the type of model actors carrying out disinformation campaigns can be identified. Regarding Authoritarian and Crisis States, Bradshaw and Howard note that governmental ministries such as cyber troops working for the Internet Research Agency in Russia are typically charged with carrying out disinformation campaigns to protect cyber infrastructure and content. Whereas Democratic states often saw members of political parties as the main actors conducting disinformation campaigns, typically carried out against domestic populations during government elections.

Another issue with determining foreign actors' involvement in social media disinformation campaigns concerns problems with the victim state's capability towards identifying the location of where disinformation attacks originate. Whereas noted before about how political groups online will typically broadcast themselves on social media publicly, foreign actors or "cyber-troops" are generally publicly funded but discrete actors or groups that utilize anonymizing technology such as Virtual Private Network's or The Onion Router to accomplish misinformation campaigns across state boundaries (Forrester, Bacovcin, Devereaux, & Bedoya, 2019; Bradshaw & Howard, 2018). In Canada, reports developed shortly after the conclusion of the 2019 Federal Election offered evidence of Russian interference, albeit at a lesser degree compared to the 2016 U.S. Presidential Election, that sought to utilize social media platforms online to drive wedge issues amongst Canadians to 'distract' Canadians from other Russian misinformation campaigns (p. 11). Utilizing the BEND Framework, specific strategies by Russian botnets and troll farms had been found to promote misinformation campaigns on core Canadian politic issues including ethical considerations, climate change, as well as the Alberta Tar Sands. For this study, the authors note that “each letter of BEND corresponds to one quadrant produced by the combination of the two axis” (p. 2). Based on existing research on disinformation and Russian information manoeuvres, the reports author’s state the BEND Framework “describes strategies that can be used by actors in the information environment” and that “information activities are characterised along two axis: community manipulation versus content manipulation and positive manipulation versus negative manipulation” (Forrester, Bacovcin, Devereaux, & Bedoya, 2019, p. 2). How these objectives were achieved typically focused on how the bots were utilized to provide positive or negative support to these issues to create division among Canadian social media users by promoting conflict online.

iii. Internet Regulation & Governance, Cyberattacks & Self-Defence

As attacks originating on the internet become more commonplace and accessible to motivated parties, an issue for legislative bodies concerns the capability of the state to adequately develop legal frameworks that are appropriate to the threat that internet-borne attacks harbor. Given the many resources available online to facilitate anonymity, attacks that leverage the internet are often difficult to trace an exact location when the perpetrator masks their location data through multiple networks globally (Stahl, 2012). Even when an attacker’s location can be traced, investigations can face complications when cyber-aggressors reside in foreign countries whose own governments are unsupportive towards international jurisdictions such as the deportation of the suspected parties to the victim state to face prosecution (Couzigou, 2014). Despite these issues, the use of existing international treaties is often hailed to be the most productive avenue to pursuing restitution from cyberattacks and it can be demonstrated that the attack originated from a foreign state or individual.

In the absence of international ad hoc treaty regulations towards the cyber dimension, scholars advocate for the use of existing treaties and customary law to outline governance on matters pertaining to cyberattacks. At the time of this writing, 2001's Council of Europe's Convention on Cybercrime (otherwise known as The Budapest Convention) is currently the only legally binding instrument of international law that addresses criminal activity in cyberspace with only 61 states having signed and ratified the treaty (Van Dine, 2020). Coming into force in June 2004, the treaty directs signatory states to "criminalize certain cyber offences in their domestic legislation, to extend their jurisdiction to offences originating from their territory or committed by their nationals, and to provide mutual assistance in investigations and prosecutions" (p. 19). While the Convention specifies prohibited conduct online, it becomes the responsibility of the signatory states to provide the elements of prohibited conduct and the most efficient route to enforcement of each state's domestic laws (Stahl, 2012). What the Convention does not achieve however, is the formal establishing of universal procedures towards prosecution and punishment for any given act. Instead, the Convention relies on the international cooperation of signatory states to assist in the enforcement of domestic law. For example, public and private sectors of Estonia suffered a devastating cyberattack that stretched several weeks following the removal of a post WWII monument commemorating the Soviet victory over Nazi Germany in the town of Tallinn (Stahl, 2012). The attack included the use of a Distributed Denial of Service (DDOS), whereby malware infected computers are leveraged to send "a massive series of data packets to the targeted networks" overloading the operational capacity of Estonia's computer networks and shutting them down (p. 256). Given how the Estonian government relies heavily on the internet for daily operations, the sabotage caused significant damages to the country including widespread unrest and rioting as critical government services were rendered obsolete in the aftermath of the attack. Following the supposed identification of the attacks originating within Russia, Stahl (2012) notes that “although the Estonian government claims to have proof that the earliest attacks originated from Russian government computers, the nature of a DDOS attack makes determining the original source of the attack difficult” (p. 257). Further complicating the investigation concerned the Russian government’s refusal to help locate and prosecute the individuals involved, which Stahl (2012) argues to show how an international approach is needed to mandate the cooperation of implicated states towards investigations that cross international boundaries especially as cyberattacks can be deployed seemingly anywhere. Following a request for military aid from NATO in responding to the attack, it was found that some of the hackers involved were not based in Russia and were based in Brazil and Vietnam (Gable, 2010). The initial reluctance to assist Estonia in identifying a possible suspect by Russia can be interpreted as reflective of the broader issue facing international efforts to combat cyberattacks. Given the Convention’s few signatories or recognition of reflecting customary international norms, Stahl (2012) argues that “a victimized nation attempting to prosecute attackers residing in a country that is not party to the Convention will have to rely on an independent agreement in order to pursue criminal charges against perpetrators located within the non-member state’s borders” (p. 264). This means that without bilateral acceptance of the Convention between the 2 states involved, the victim state would be forced to resort to criminal prosecution under the origin states jurisdiction and is not guaranteed as the nebulous nature of the term “cyber” may not be considered criminal for prosecution such as in the Philippines (Gable, 2010).

Attempts to help deter cyberattacks against critical infrastructures in the literature focus on the application of an international legal framework similar to UN treaties such as the United Nations Convention on the Law of the Sea (UNCLOS) which governs legal relationships related to the sea such as the sovereign states duty to combat piracy outside of their own jurisdictions (Stahl, 2012; Gable, 2010). Given how the Convention only outlines directives to signatory states to cooperate and implement domestic legislation on prohibited cyber-conduct, international agreements rely on the ‘Martens Clause’ to adapt existing international law towards the cyber-dimension. Contained in Article 1(2) of Protocol I Additional to the 1949 Geneva Convention, it states that:

> [i] n cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience

This means that in the development of new warfare technologies that are not prohibited explicitly by international treaties does not expressly permit their lawful usage. Rather, the clause can be used as an extension of existing prohibition or regulations towards new weaponry to avoid gaps in legislation (Van Dine, 2020). However, Van Dine (2020) contests that the application of this clause towards cyberoperations “is that they do not take into account their uniqueness and might prove to be too general” (p. 23). This is largely due to how Martens Clause also facilitates the extension of existing treaties notion that imply the existence of territory or geographical borders that fall under state sovereignty, whereas cyberspace can be inherently borderless and subject to constant change.

While some nations have become better equipped to allow their citizens the ability to use the internet relatively safely, establishing effective regulations becomes increasingly problematic as these same nations often hold conflicting views on appropriate responses to disruptions (Kierkegaard, 2005). Further complicating an international agreement on the regulation of the internet is that by its own nature, the internet itself is something that does not have a singular, authoritative body and can transcend international boundaries or laws. While some international agreements do exist in differing capacities, organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN) or the International Telecommunication Union (ITU) primarily deal in matters relative to URL domain registration or formulating technical standards for information and communication technology respectively (Take, 2012). Regarding international relations, it is often noted that the influence a nation carries with it will generally influence how foreign governments will react when a citizen or group residing in their borders is sought for damages (Take, 2012). Given its capabilities, drafting policy relative to cyberattacks conducted in foreign locations requires a form of legitimacy between stakeholders and can be exercised during the entire process of outlining international internet regulation between governments. Take (2012) describes three processes that influence the legitimacy that a government holds during policy drafting/implementation which includes the input, throughput, and output legitimacy, and the success of cybercrime policy between nations rests on the strength of the normative and empirical legitimacy an international information technology regulator has during each three processes. Take (2012) defines the “input” measure of legitimacy to the effect of how involved all relevant stakeholders in policy matters are included in the decision-making process, the “throughput” legitimacy refers to the accountability of the decisionmakers involved, and the “output” legitimacy measure as the ability of governance arrangements power in convincing internal and external stakeholders to accept regulations.

Further concerns relative to international governance on information technology rest on policies implemented through the United Nations including laws that govern how cyberattacks can breach a nation’s sovereignty and whether they satisfy conditions to warrant self-defence. The capabilities of augmenting or developing original attacks through the internet can allow interested actors to launch attacks virtually to precise locations while facilitating anonymity of their own location ultimately hindering state retaliation (Couzigou, 2014). Furthermore, given the growing complex nature of the internet and its affordance in anonymity, it has become increasingly difficult for victim states to claim that the perpetrators were directed by state authority to conduct the attacks. Plausible circumstances imposed by international law that hinder investigations include providing evidence that the actor was situated within the foreign state, the individual or group was empowered by that state government (typically through legislation), or the individual was acting under the instruction, direction, or control of the state (Couzigou, 2014; Bradshaw & Howard, 2018). The international law to self-defence, located in article 2(4) of the UN Charter, and the lack of a written description of what categorizes force is oftentimes debated as to its function relative to cybercrime (West, 2018). Furthermore, problems arise when attempting to incorporate cybercriminal acts as either ‘instrument-based’ or ‘consequence-based’ models of force, as the utility of an IT system can potentially fall into either category. Couzigou (2014) argues that the user of IT devices in attacks ought to be classified as a form of consequence-based use of force, as this allows a wider degree of interpretation when clarifying cybercriminal behaviour as either an act of armed force or an armed attack. While the use of an IT device is required, the consequential effects of the attack would require serious consideration as to whether it would be classified as a state enabled use of force or attack and thus warrant self-defence.

iv. Digital Privacy & The Charter

The purpose of this section in the literature review will aim to provide a comprehensive summary of scholarly works that examine Canadian courts and jurisprudence towards the role of digital privacy amid growing state surveillance and new avenues towards data harvesting via a proliferation of devices becoming increasingly connected to the internet. This includes a brief overview of scholarly works that examine s.8's expansion into a digital era via a variety of case decisions and whether the Charter is adaptable to growing technologies. This section will also examine the expansion of state powers for national security purposes via 'big data' surveillance, otherwise known as metadata, and its controversial nature towards digital privacy. This includes examining the recent ruling against CSIS concerning their "Operational Data Analysis Center" (ODAC), a bulk metadata analysis program that had been in operation since at least 2006. Finally, this section will conclude by examining the role of IoT technology as it pertains to individual security risks and the normalized diminishing of privacy rights online as modern technology devices become increasingly connected to the internet.

While the right to informational privacy is not explicitly enshrined in the Charter, it has been given constitutional status in Canada via the expansion of certain rights pertaining to the right to be secure against unreasonable search or seizure (s.8). Earliest interpretations to s.8 were situated on jurisprudence that focused on the protection of property rather than the individual, and it wasn't until *Hunter v. Southam* (1984) that s.8 transitioned to be reflective of "people not places" and that the interest at stake was against privacy, not property (Austin, 2007). Austin (2007) further notes that this decision helped to set s.8 jurisprudence "within a framework suitable for the modern world, where the paradigm for unjustified state intrusions into individual lives is not the knock of the king's messengers at one's" (p. 499). Further cases heard by the Supreme Court refined the decision in determining what types of information trigger s.8 protection such as *R v. Plant* (1993) that introduced the concept of a "biological core" defined as information "which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" (p. 283). These two decisions predicated other decisions that would shape s.8 jurisprudence in Canada for subsequent decades. Against the backdrop of emerging technologies afforded to state surveillance however, scholarly opinion towards the effectiveness of s.8 jurisprudence in protecting individual privacy interests is mixed. While Austin (2012) argues that jurisprudence towards s.8 protections highlight a lack of effectiveness against emerging forms of surveillance, she considers the notion that privacy interests against state surveillance following *Southam* and *Plant* as being "absolute" and its infringement ends the policy debate rather than it being a part of the broader conversation in public policy. She advocates that traditional rule of law interpretations that only address "reasonable expectations" of privacy have worked to narrow its applicability and allow the unfettered expansion of state surveillance powers rather than constrain it. To illustrate this, she notes *R v. Gomboc* (2010), which saw the courts side with the state on permitting the surveillance of electrical usage patterns via a digital recording ammeter (DRA) as the accused had not requested their utility company to refrain from sharing their data with law enforcement. In this case, the courts had affirmed that privacy interests were not infringed as the accused had not exercised their ability to have their data kept confidential which Austin (2012) argues had failed to consider other elements to the rule of law including the ability for the state to simply enact legislation that make the intrusion lawful. In contrast, Conrod (2019) notes that while s.8 jurisprudence has afforded the right tools to protecting individual privacy interests, these decisions have failed to provide certainty or predictability when dealing with the rapidly growing technological environment. She cites the competing deliberations made by justices on the Supreme Court in *Gomboc* on what constitutes information relative to the "biographical core" when utilizing surveillance technology such as the DRA as creating confusion amongst lower courts when applying the same tests to determining whether a method used warrants s.8 protections. To counteract this, Conrod (2019) proposes that a spectrum of privacy protection specifically dealing with technology be considered when determining s.8 breaches of state investigations. Given the rapidly evolving nature in technology both new or developing, privacy interests occur at varying degrees when using them and can allow the courts to better follow a case-by-case basis when balancing them against the surveillance methods used by the state in their investigations.

Following the Snowden revelations, it became increasingly clear just how critical a role "big data surveillance" (BDS) has in the facilitation of national security operations despite its controversial nature as it relates to digital privacy. Whilst most documents leaked pertain to the United States' National Security Agency, Canada's own national security agencies were implicated in findings that indicated international cooperation amongst other allied Five-Eyes agencies in conducting big data surveillance sparking public outcry (Lyon, 2015). Big data surveillance refers to the "control over collection, storage, and processing infrastructures in order to accumulate and mine spectacularly large amounts of data for useful patterns" (Andrejevic & Gates, 2014, p. 190). Emerging from the aftermath of the 9/11 terrorist attacks, big data surveillance represents a shift in national security agencies investigations from being deliberately targeted against individuals of interest towards a broader, proactive approach that seeks to harvest as much data online as possible and work inward. This form of surveillance involves the use of secretive programs that at times require the cooperation of public and private sectors including internet providers in collecting data no matter the relevancy to investigations (Laurin, 2020). Prior to the Snowden revelations little was known about the existence or capabilities of these programs, but Lyon (2015) notes that the revelations had brought secretive programs to light and that their true capabilities far exceeded scholarly concerns. Examples of techniques used by agencies include the use of interceptors, which are placed along cable routes to facilitate mass data collection for future analysis including ‘Levitation’, a program used by CSE to gather data from up to 15 million downloads from file sharing websites (Lyon, 2015). At the centre of big data surveillance concerns the usage of specific anonymized portions of metadata, and while it holds substantial value in the success of proactive national security agencies internationally, it’s utility in identifying individuals based on algorithmic inferences has been noted by scholars as being detrimental to both human and privacy rights (Lyon, 2015; Laurin, 2020). Metadata represents anonymized digital footprints that one creates when browsing the internet or using telecommunication devices and can be exploited by metadata harvesting programs for national security purposes including the identification of potential individuals of interest (Lyon, 2015; Roach & Forcese, 2015). Examples of metadata that can be used for national security purposes include vehicle identification numbers, telecommunication timestamps including the date, time, and general location of where the call occurred. A prominent argument against the use of metadata in national security concerns how the previously mentioned expansion of BDS techniques have been reframed by government agencies as being lawful despite the secrecy in how BDS is carried out (Austin, 2015; Laurin, 2020). Following the Snowden leaks, Austin (2015) argues that the secrecy in which national security agencies engage in BDS precludes any insight into whether these programs conform to the rule of law. Defined as ‘lawful illegality’, she further argues “the problem is that the plausible legal interpretation is one provided by the government itself and its conclusion of lawfulness is far from obvious to an outside observer” (p. 107). In the case of the ODAC decision against CSIS, Laurin (2020) notes that the agency may have potentially engaged in misleading federal oversight parties about the true potential of the metadata harvesting program, and that by using carefully selected terminology it had deterred any investigation as to whether the irrelevant data subject to exploitation had been kept legally.

Outside of Canadian court jurisprudence and Charter protections, another element surrounding digital privacy concerns itself with previous statements made here towards the evolving ecosystem of IoT technology, social media platforms, and growing state capabilities to conducting digital surveillance facilitated via the expansion of internet access internationally. This includes scholarly discussions towards the growing accessibility of SMART technology and how permissions needed to facilitate the use of their features has been increasingly encroaching Canadian privacy interests online. Considering the evolving capabilities of traditional technology and the integration of SMART features, recent advancements in this space have created new avenues including both in convenience to the user as well as new methods to data harvesting. Regarding the IoT, Maras (2015) notes that “in its the most basic sense, the IoT refers to the connection of everyday objects (eg TVs, appliances, and exercise equipment) to the Internet. It enables the real-time monitoring and vast collection of data about property, people, plants, and animals” (p.99). The connection of traditional technology to the internet provides a multitude of benefits that include the ability to remotely control products such as HVAC systems, real-time monitoring of health such as the use of fitness trackers, as well as the ability to monitor vital signs in medical settings such as the integration of the internet to radiological machines, all of which can be connected to any Wi-Fi or cable access points. Maras (2015) further notes that the prevalence of IoT technology has also afforded the ability for “machine to machine” (M2M) communications, whereby devices are able to “translate data according to context and make relevant, timely, and valuable decisions based on readings” (p.100). Important to note here however, is that these seemingly tangible benefits towards efficiency have also come with a substantial cost, namely, that most IoT technology is developed without security or privacy in mind and prone to exploitation (Conrod, 2019; Maras, 2015). These costs can include the lack of proper security measures in medical equipment (allowing backdoor access and manipulation) or existing vulnerabilities of these devices that can be breached remotely causing substantial losses. Canada’s own intelligence agencies have also noted this trend, as recent reports have indicated that the growing integration of Canada’s critical infrastructures to the internet have also opened avenues for aggressors to conduct sabotage virtually via the use of malware including ransomware towards hospitals or electrical grids (CSE, 2018; CSE, 2019). Additionally, as more devices become integrated into the IoT, they can have severe impacts towards the expectations of privacy that users may have when using products but are forced to do so to continue their usage of certain products (Conrod, 2019).

METHODS

i. Introduction

For this study, the qualitative data analysis (QDA) methodology as outlined by Saldana (2014) was employed to analyze Canada's national security relating to digital threats in the current threat environment. This included the preliminary identification of datasets and gathering relevant materials to assist in sourcing archival datasets that would be appropriate for qualitative data analysis. Following the review of Canada's process in developing/implementing legislation and reviewing other similar bodies of research focusing on Canadian legislation, the committee meeting's transcribed testimonials and submissions that preceded the 'locking in' of C-59's overall structure and mandate were identified as the primary source of qualitative data to this research project given that these meetings had utilized expert witnesses in occupational roles that were of interest to national security objectives. Per the then Public Safety Minster Hon. Ralph Goodale, C-59's deliberations were highlighted to be given special interest that allowed the bill's scope to be modified between the first and second readings instead of only being locked after the first reading. Since these transcribed meetings and briefs are digital in nature and can be readily found online via the Government of Canada's website for Parliament (https://www.parl.ca/LegisInfo/en/bill/42-1/C-59), it was determined that these archival documents be examined. This methodology afforded this thesis the capability to procure qualitative datasets in a non-intrusive manner, thus facilitating the ability to revisit past datasets for reflection, re-coding, and early analysis pertinent to Microdeviation theory and technosocial implications.

The justifications for utilizing qualitative data analysis in this research can be found both in Saldana's (2014) own methodology and other scholarly contributions to conducting QDA, as well as through demonstration of prior scholarly research that has focused on both Bill C-59's earlier legislative drafts and prior provincial attempts to legislate certain cyber elements of crime including cyberbullying. The integration of QDA for the purpose of this thesis allows for an intimate approach to exploring the vast amounts of testimony and submissions that were made pertaining to C-59 and identifying nuances that contributed toward establishing the mechanisms present within the bill. As Saldana (2014) has referred to in his various publications on QDA, integrating this methodology affords constant revisiting, refining, and analytic foresight. Qualitative analysis can explore possible implications of microdeviations on a national (and at times, international) scope. Finally, the utilization of QDA for the purpose of this thesis will also allow for a far more expansive commentary on the technosocial implications that can arise from this seemingly apparent "digitalized arms race" that could not effectively be integrated into a quantitative study.

In other scholarly publications, qualitative methodologies were also used to examine both the preliminary implications of C-59's new powers as well as other provincial attempts at legislating cyber elements of crime, notably with cyberbullying. During the initial unveiling and early discussions surrounding C-59's terminology, West (2018) integrated the legislation's earlier drafts, public official commentary on the bill, as well as archival publications of CSE activities abroad. These data were contained in the Snowden revelations and identify the international implications of cyberactivity authorization as it pertains to the United Nations Charter concerning civilian rights, compliance with International Humanitarian Law (IHL), and the resulting possibility of retaliation from other member states towards cyberoperations that could implicate the civilian agency as war combatants. Additionally, Parsons et al. (2017) on behalf of Citizen Lab had also researched and published their first report concerning the new powers to be implemented in C-59. This report was submitted to the Committee for consideration on proposed amendments to C-59 and other priority aspects of the legislation needing to be addressed. In their report, Citizen Lab focused on the new mandates being proposed in the CSE Act of the legislation as well as the review powers being implemented with the integration of the National Security Intelligence Review Agency (NSIRA). The lab's objectives were achieved primarily through a comparative analysis of C-59 to other previous national security acts including the bills predecessor that was enacted by the Conservative government, Bill C-51. A final study concerning the Provincial Government of Nova Scotia's legislative attempts to combat cyberbullying by Taylor (2016) had also utilized similar qualitative methods and data sources to provide a qualitative case study on the abrupt striking down of the *Cyber Safety Act*. This study included the analysis of the judicial decision surrounding the growing complexities of legislating digitalized behaviour as the commentary from striking the Cyber Safety Act noted that the protection of Section 2 Charter rights extended as well to communications made online.

ii. Sample Identification

For this study, the recorded committee meeting minutes available to the public on the Canadian Parliament website were selected as they provide accurate accounts of both the selected expert witnesses as well as cross examinations by the members of parliament that comprised the Standing Committee on Public Safety and National Security (https://www.ourcommons.ca/Committees/en/SECU/StudyActivity?studyActivityId=9807256#DT20171130SECUMEE88ID9807256). This resulted in 16 committee meetings that were then imported to NVIVO and subject to a narrative assessment by querying key terminology relative to the digital and social elements contained in C-59. This brief assessment of the testimonies contained in the meetings allowed for a filtering out of unnecessary reports where their contents held no substantial value to the overall goals of this study. In total, 13 dates where meetings were held by the committee split into two 2 ½ hour blocks for a total of 26 hearings were identified as relevant for the study. Following the acquisition of the relevant meetings to this study, the briefs that were submitted by the expert witnesses that testified were also collected and added to the NVIVO project for coding and analysis. The primary reason for their inclusion is entirely supplemental, as the briefs contain a more in-depth qualitative focus to their respective proposals revising C-59 and any forthcoming concerns of certain legislative powers that informed the ensuing analysis of this study. With the little time that is allotted to both members of the committee to examine expert witnesses and how briefly at times testimony may be, examinations on certain digital matters of C-59 were often cut short of a definitive answer. However, what was often the case when this occurred was that witnesses were asked to supplement their briefs provided to the committee with more detailed responses for the committee's consideration. In total, 10 text briefs were submitted by expert witnesses that provided a much more expansive insight on their respective proposals to legislation amendments and concerns relative to the digital elements of the bill. These datasets were then stored on a USB drive with frequent uploading to a OneDrive to ensure data integrity and prevent accidental deletion.

These datasets were then subject to an initial coding procedure with codes that were pre-determined based on both the tenants of Microdeviation Theory and supplemental codes that were derived from concepts contained in the scholarly sources used in the preceding literature review as shown in Figure 3.1:

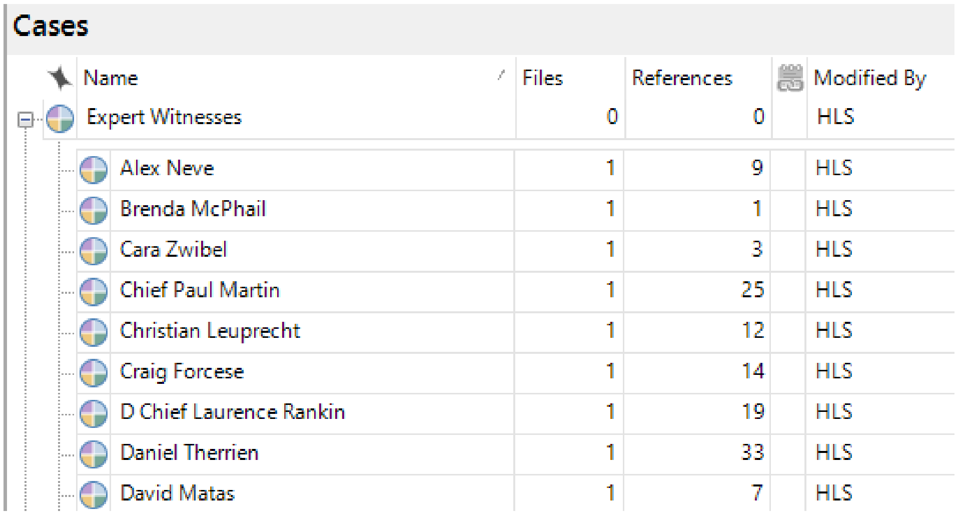
Charter Rights

Cybercrime Legislation as it Encroaches Charter Rights	References that focus on how legislation concerning cyber measures affect Charter Rights.
Concerns Relative to Individual Privacy	
Balancing privacy concerns to national security	References that consider matters relative to an individual’s privacy stakes and how national security mandates may affect it.
Privacy of Canadians from Cyber Search / Seizure	References to testimony focusing on protecting Canadians from cyber-searches in the context of national security investigations.
Canadian Metadata Complexities	References that focus on matters pertaining to metadata and its usage in national security investigations (including justifications for its continued use).
Cyberoperations	
Defensive Cyberoperations	References that focus on the **DEFENSIVE** capabilities of cyberoperations, and any other references that include the term.
Offensive Cyberoperations	References that focus on the **OFFENSIVE** capabilities of cyberoperations, and any other references that include the term.
Cyber Cold War	References that consider concerns of a growing 'Cyber Cold War' from enabling cyberoperations.
General Descriptors RE: Internet	
Canadian National Security Responses Compared to Five Eyes Allies	Includes references that focus on testimony or questioning that situates Canada's national security responses to that of other Five Eyes allies.
Cyberconflicts on the World Stage	Include references relative to: a) "The New Cold War" b) Warfare categorized as being fought on keyboards instead of traditional weaponry c) International incidents involving the use of digital technology (i.e., Stuxnet)
Internet as an Emerging New Threat to Canadian National Security	References that contain matters of the internet as becoming more novel in its use towards conducting cyber-attacks, recruitment, disinformation etc.
International Implications	
Civilian agencies as an extension of the military	References that allude to the implications of civilian agencies and their operatives as actants of war.
Cyberoperations as a breach of international boundaries	References to how legislating cyberoperations can breach international boundaries and potentially be regarded as acts of war.

Microdeviations	
Normalization of Digital Deviancy & Annoyances	References that use terminology or outright explanations that situate elements of internet/technology as being normalized such as diminishing privacy interests to continue using certain products, or the willingness to accept disinformation online as a part of the contemporary internet structure.
Moral Panic	Catch-All header for the various forms of moral panics relative to internet or digital technology.
Changing Face of Contemporary Terrorism	References that focus on the shifting ways that contemporary terrorist groups operate.
Foreign Espionage or Sabotage	References to testimony relative to national security when it concerns new threats of foreign governments (i.e., Russia)
Internet Futures-Lagging Legislative Response	References to testimony that indicate a gap in legislative responses to growing digital threats.
Lawlessness of the Internet	References that consider testimony that frames the internet as being a place that holds no formal regulation, in need of intervention etc.
Disproportionate Legislative Responses	References that focus on the potential for impacts that go far beyond the scope of what the legislation targets.
Review Agencies	
Intelligence Commissioner	Focused on components of the bill referring to the Intelligence Commissioner.
NSIRA Review	Focused on components of the bill referring to the National Security Intelligence Review Association.

Figure 3.1: Initial codebook with descriptions

To properly facilitate the evaluation, identification, and revising of proper thematic categories, the Critical Appraisal Skills Programme (CASP) Qualitative Studies Checklist was utilized for each individual academic source when determining whether these codes were sufficient for this thesis (Critical Appraisal Skills Programme, 2018). Given the nebulous nature of cyber elements especially as it relates to national security, this was done to ensure that the codes generated were reflective of scholarly, law enforcement, and political perspectives towards the digital powers being granted in C-59. The CASP Qualitative Checklist functions as an appraisal tool for qualitative sources by examining 3 broad issues including whether the results of the study were valid, what the results were, and if the results are assistive in a local setting. While the use of a scoring system is discouraged, the checklist helps users to filter out irrelevant sources whose results are unrelated to the research in question by drawing out the qualitative significance in others. 10 questions of each source representative of the 3 broad issues help the researcher to synthesize the results of each potential source and compare or contrast them to other sources. A total of 20 unique identifiers were subsequently used to properly represent attributes found in the testimonial accounts and briefs by expert witnesses and members of the committee. These codes were then clustered into similar, overarching themes contained throughout the datasets to better illustrate the forthcoming analysis. The initial project contained 7 clusters that included the identifiers focusing on themes of general descriptors of the internet, digitalized individual privacy concerns, and the advent of potential cyberwarfare from a digitalized cold war (see Figure 3.1). During this initial coding, NVIVO’s case function was utilized to capture testimonial data and attached to unique identifiers to represent each expert witness or committee member to maintain data integrity. NVIVO’s case classification function allows researchers to generate identifiers that can properly classify qualitative information as belonging to a select individual, in this case, case classifiers were generated for each expert witness and committee member involved in C-59’s deliberations (See Figure 3.2). Furthermore, each case classification was assigned an occupation modifier to help differentiate industry alignment between expert witnesses for potential further analysis. An example of this function was to differentiate expert witnesses from the academia field or certain branches of government including national security or the criminal justice system.



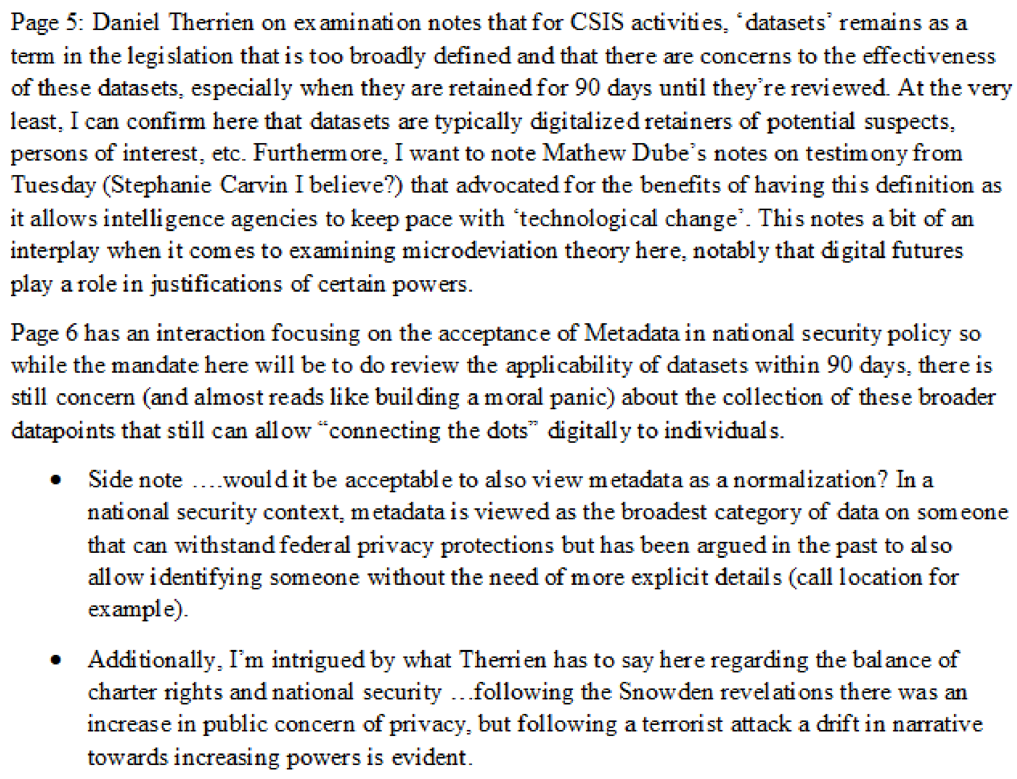
Cases

Name	Files	References	Modified By
Expert Witnesses	0	0	HLS
Alex Neve	1	9	HLS
Brenda McPhail	1	1	HLS
Cara Zwibel	1	3	HLS
Chief Paul Martin	1	25	HLS
Christian Leuprecht	1	12	HLS
Craig Forcese	1	14	HLS
D Chief Laurence Rankin	1	19	HLS
Daniel Therrien	1	33	HLS
David Matas	1	7	HLS

Figure 3.2: Example of NVIVO's Cases Function

Following this initial coding procedure, a secondary 'focusing of codes' was conducted similar to Saldana's (2014) methodology with the objective of combining similar or lesser used codes together to prevent the study from spreading analytical implications too thin and to strengthen the forthcoming analysis of codes that were comparatively stronger or provided more value to discussions focusing on theory testing. This resulted in the condensing of the 7 clusters initially identified into 5 more concise themes as well as the combining of the initial 20 codes into 11 to facilitate a more meaningful analysis. Furthermore, during both coding procedures of this study these datasets we're also subject to brief analytic memos that contained personal insights towards potential theme relationships, frequencies of similar topics contained in witness and committee member dialogue, and early draft ideas concerning the resulting implications towards Microdeviation Theory and technosocial scholarship. An example of these forms of analytical insights can be viewed below, where an examination on the December 7, 2017, meeting focusing on the definitions of "datasets" and their need to be broadly defined to keep pace with technological advancement was briefly analyzed as both a potential for disproportionate legislative responses and the normalization of expansive metadata surveillance

(Figure 3.3). The finalized project contained a total of 13 committee meetings comprised of 26 hearings, 53 expert witnesses examined by 19 committee members (10 Liberal, 8 Conservative, 1 New Democratic Party) for a total of 495 pages (318 pages of committee meetings and 168 pages of briefs).



Page 5: Daniel Therrien on examination notes that for CSIS activities, ‘datasets’ remains as a term in the legislation that is too broadly defined and that there are concerns to the effectiveness of these datasets, especially when they are retained for 90 days until they’re reviewed. At the very least, I can confirm here that datasets are typically digitalized retainers of potential suspects, persons of interest, etc. Furthermore, I want to note Mathew Dube’s notes on testimony from Tuesday (Stephanie Carvin I believe?) that advocated for the benefits of having this definition as it allows intelligence agencies to keep pace with ‘technological change’. This notes a bit of an interplay when it comes to examining microdeviation theory here, notably that digital futures play a role in justifications of certain powers.

Page 6 has an interaction focusing on the acceptance of Metadata in national security policy so while the mandate here will be to do review the applicability of datasets within 90 days, there is still concern (and almost reads like building a moral panic) about the collection of these broader datapoints that still can allow “connecting the dots” digitally to individuals.

- Side note ….would it be acceptable to also view metadata as a normalization? In a national security context, metadata is viewed as the broadest category of data on someone that can withstand federal privacy protections but has been argued in the past to also allow identifying someone without the need of more explicit details (call location for example).
- Additionally, I’m intrigued by what Therrien has to say here regarding the balance of charter rights and national security …following the Snowden revelations there was an increase in public concern of privacy, but following a terrorist attack a drift in narrative towards increasing powers is evident.

Figure 3.3: Memo analysis example taken from the December 7 2017 meeting

iii. Analysis

The analysis of this research seeks to implement strategies similar to preceding academic work that examined both C-59’s early stages as well as legislation prior including C-51. For the purpose of discussing national security legislation in a Canadian context, this research was particularly interested with how these new mandates that are motivated by the modernizing of Canada’s national security legislation can indirectly expose drastic implications on international relations. As mentioned previously, publications from The Citizen Lab (2017) and West (2018) both demonstrated that qualitative studies can indeed bring into focus the seemingly out of reach yet very plausible ramifications that cyber-empowerment of national security agencies can have on future theatres of war, especially with regards to how Canada positions itself alongside United Nations members.

Alongside the 2 waves of coding, iterative memos were frequently drafted that focused on bringing out the more abstract sources of qualitative data for this projects analysis. For clarity, this meant making memos concerning an array of topics that focus not only on how certain testimonial accounts from expert witnesses frame the objectives of C-59 with concerns to international relations or Canadian Charter rights, but also included notes referring to the exchanges made from committee members. This included (but not limited to) frequent reflection on the tone of how certain questions were asked, the negotiations and balancing of Charter rights as they referred to the context of national security, or how the new mandates contained in C-59 could be justified in contemporary society. Saldana (2014) notes that these forms of analytic memo writing help to bolster both creative thinking of the project's objectives, but also inform a projects analysis by allowing the user to begin generating ideas early on in the research process and facilitate the revisiting/revision of codes in order to bring about more substantiated arguments.

Given the nature of this research, it was vitally important to establish a codebook at the onset of qualitative data analysis. Rather than letting the data generate themes/codes similar to grounded theory, 3 initial themes reflective of the 3 main objectives to Microdeviation Theory (normalization, manufactured uncertainty, disproportionate legislation) were developed and added to the codebook at the onset of QDA while letting other themes emerge inductively. As such, while certain codes identified in this study were given flexibility to be revised if needed it was important from the onset that the codes used objectives outlined by Popham (2018) in Microdeviation Theory and that they be given priority when examining the datasets. Furthermore, given the 3-stage trajectory that Microdeviation Theory establishes to warrant its utility this meant that evidence throughout the datasets had to sufficiently contain testimonials for each of the 3 aspects. Whereas those themes were solidified prior to conducting QDA, other themes that were established reflecting key properties of the bill (including CSE cyberoperations and unifying Canada's national security review mechanisms) were given partial latitude to be modified in future reflections. Given C-59's sweeping nature in fundamentally changing Canada's national security agency structure, themes focusing on the Cyberoperation mandates of the newly enacted CSE act as well as the salient testimonials concerning the overhaul of both SIRC and the CSE Commissioners office into the NSRIA were also given priority in qualitative data analysis as the forthcoming discussions on these themes will show.

iv. Results

The results of this methodology helped to establish a sophisticated NVIVO document that itself contains a dataset with the multitude of themes that were persistent throughout the legislative process leading to C-59's formal ratification in June 2019. Furthermore, this dataset also contains a case management suite that includes indicators regarding the occupational and political affiliation of expert witnesses and committee members respectively. This includes identifiers regarding expert witness qualifications as well as information that briefly highlights the industries and employers each witness represents. Additionally, this also included attaching testimonial evidence to their specific expert witness that assists in categorizing and potentially informing qualitative analysis that can focus on their significance to the overall debates regarding C-59's contents. 51 expert witnesses were identified from 5 different industries across Canada representative of 24 different employers ranging from national security agencies (CSE/CSIS), civil rights groups, as well as individuals appearing either on their own or representing academic universities in Canada. Finally, 20 members of parliament that established the committee were also identified with political affiliation from the Liberal Party of Canada (10 members), Conservative Party of Canada (8 members), and the New Democratic Party (1 member).

v. Limitations

Given this thesis' stated research objectives, the primary limitation to this work concerns a pre-established negligence to the inclusion of other facets of C-59 that include meetings focusing on other aspects such as the reconciliation of C-51's expansion of the No-Fly List and secret courts or the revision of the previous advocating-terrorism offence. This meant that while this thesis' results will have bias on concerns relative to cybersecurity and expansion of digital powers, that a broader discussion surrounding other aspects of the bill are precluded here from analysis. Furthermore, the utilization of QDA also precludes this study from formally exploring a quantitative approach to examining possible correlations amongst the varying degrees of testimony contained and determining if any measurable impact exists towards C-59's finalized structure. Additionally, focusing this study specifically to the meetings surrounding C-59 results in the exclusion of other government meetings and publications surrounding C-59 that took place during the same time that may have focused on specific aspects of legislation including the Standing Committee on Access to Information, Privacy and Ethics.

FINDINGS

i. Introduction

In total, the dataset contains thirteen primary meeting minutes that were identified as having sufficient testimony relative to this thesis while also including ten secondary witness briefs for a total of twenty-three qualitative datapoints for analysis. The page total of the primary datapoints contained 318 pages, while the secondary datapoints comprised of 177 pages for a complete sum of 495 pages of data. From these twenty-three datapoints, the entirety of codes identified throughout this research contains a total of 520 references pertinent to the different themes that were present and can be viewed in the Appendix A.

While the following sub-sections will examine each component's findings in greater detail, this section will provide a general overview concerning how Microdeviation Theory was tested and what evidence contained in the dataset supports the possibility of microdeviation presence. To test the integration of Microdeviation Theory in relation to C-59's deliberations, the committee deliberations were deductively assessed for thematic evidence in alignment with microdeviation including normalization, moral panics, and disproportionate legislative response. The thematic approach also allowed for exploratory analysis of additional themes outside of Microdeviation Theory as supplemental towards this projects analysis. This included the identifying of four key themes that included considerable focus on C-59's relation to Canadian's expectation of privacy rights online, the examinations that focused on the newly implemented NSIRA and their capabilities to monitor 3 NSAs, as well as the bigger theme surrounding concerns relative to the new powers being granted by C-59, the most notable surrounding the new active/defensive cyberoperations powers being added to the CSE's mandate. The following pages will further provide commentary on the most salient of findings that emerged from these meetings while also providing supplemental excerpts of specific exchanges and examples of testimony made to further bolster the fourth-coming analysis.

ii. Findings V1.1: Microdeviation in C-59

At the onset of data analysis, three initial themes were defined, reflective of the three core components of Microdeviation Theory as outlined by Popham (2018). First, a theme was identified to reflect occurrences of testimony where cases of normalization in seemingly banal but deviant forms of digital conduct were present. A second theme was then generated to capture data that encapsulated potential displays or attempts at inducing moral panic regarding digitalized deviances or as Popham (2018) refers to as “internet futures”. And lastly, a third theme was generated to reflect testimonial experts that primarily focused on the seemingly disproportionate measures contained in C-59. Each of these components are prescribed in Microdeviation Theory.

Referring to Popham’s (2018) explanations of normalization, he argues that the deviant elements of the internet and technology that are relatively commonplace for a typical user include seemingly banal or generally accepted facets of deviant online behaviours including the presence of unwarranted solicitation via email (spam/phishing) or the utilization of “fake news” or “troll bots” that seeks to “obfuscate historical accounts of events or ideas through manipulation of records” (p. 161). For the purposes of this study, the definition was applied here without much alteration while also seeking to expand on the elements discussed in microdeviations regarding the topic of acceptance among a populace regarding digital data collection and astroturfing online. In other words, part one is that every day online behaviours, which we typically wouldn’t tolerate during in-person interactions, have become so common that people tend to overlook them. This is where the language about “defining deviancy down” comes from. This meant that in order to be properly codified as a form of normalization, narratives or testimonial accounts needed to discuss perspectives relative to the idea of topics such as mass surveillance, social media disinformation, and the supposition that the public holds attitudes that are dismissive of or accept digital nuisances.

At this time, it’s important to note here the more general observations regarding narratives reflective of this theme. Of the twenty-two references found in the dataset that were codified as a form of normalization, it was found that the main area of concern regarding normalization focused on two core aspects. First, a sense of naivety amongst Canadians about data collection policies online, and second, the broader cultural impact that astroturfing has towards national security objectives. This included discussions both from the committee members as well as from expert witnesses surrounding the growing integration of social media platforms and smart technology devices into Canadian’s social lives, and the perceived lack of understanding towards those platforms terms and conditions documents that dictate what forms of data can be collected and stored for future use.

The second deductive theme assessed the meetings testimony by expert witnesses for evidence of moral panics, aligning with Popham’s (2018) arguments about manufactured uncertainty and digitalized insecurity pertaining to technological developments outpacing legislative reach. While this theme typically focused only on narratives that utilized evocative language meant to garner anxiety or fear regarding a supposed lawlessness of the internet, what was of peculiar interest in this study is how these narratives were noted to branch into three predominant sub-themes: the digital advancements being made in terrorist groups both foreign and domestic, certain sub-elements of the types of sabotage or espionage conducted by foreign states, and most notably the idea of Canada’s national security legislation regressing in response to “internet futures”. Of the 148 instances where language indicative of moral panics occurred, 78 references were noted to have utilized fears of a lagging legislative response to contemporary technological development to advance some of the more controversial aspects of C-59 including cyberoperations.

Lastly, the concluding theme of microdeviation are the resulting legislative responses that can be regarded as having disproportionate implications outside of envisioned parameters. Popham (2018) notes that this typically occurs following the presentation of moral panics towards unknown facets of internet subcultures or the proliferation of technological development that can elicit calls for immediate sanction or regulation. This means that the legislative responses being introduced carry with it the possibility of granting legislative empowerment that far exceeds their discernable harm. This can include Nova Scotia’s Cyber Safety Act as an example, while more recent domestic and global legislation like the 2011 Stop Online Piracy Act (SOPA), or 2019 Article 13 of the European Union Directive on Copyright in the Digital Single Market might also be considered. While the purpose of this thesis is not to undermine the legislative responses needed with an ever-evolving digitalized threat environment, it’s necessary to highlight the concerns brought into testimony over C-59’s overhauls and digital empowerment of Canada’s national security agencies. Initial feedback on C-59's earlier drafts by Parson's et al (2017) and West (2018) provide scholarly examples of this theme when considering the international implications that can occur relative to the expansion of CSE's mandates to include active and defensive cyberoperations. Most notably, these studies highlighted how the lack of codifying cyberoperations in legislation can carry with it the potential to be considered as acts of war against pre-existing United Nations treaties pertaining to self-defence. As such, this study considered instances throughout C-59’s deliberations that focused on the perceived impacts towards both Canadian Charter rights as well as the possibility of international retaliation towards operations carried out by both civilian and military agencies.

Theme One: Normalization of Digital Deviance

As mentioned above, Popham's (2018) Microdeviation Theory considers normalizations in digital spaces to include relatively banal but also deviant facets of the internet that are subjected to a general acceptance and relegated to aspects consistent with typical internet usage. This pattern of normalization further drives its acceptance among internet users who can become apathetic to attempts at legislating digital deviant behaviours. Alongside the relatively harmful yet avoidable nature of something such as unsolicited emails, Popham (2018) also notes that efforts to manipulate narratives online such as through technological revision/astroturfing (MacLean 2008) have also been subject to further normalization and acceptance.

Given this definition, the meetings considering C-59's mandates as well as supplemental briefs given by expert witnesses were examined for instances of testimonial or cross-examination evidence that contained narratives or structures consistent with an element of normalization or inattention by Canadians despite the deviant element of possible harm. Ideally, evidence would be considered a form of normalization when narratives such as "taking common technological advancements for granted" or "Canadians lack the appreciation or knowledge of how certain parts of the internet function" were present. This resulted in the capturing of 22 instances whereby these forms of normalization had occurred.

Regarding the normalization of digital deviancies online, one such aspect considers testimony made by expert witnesses that allude towards a growing naivety of Canadians' considerations of the threat that the cyber domain has against national security. This includes both the appreciation of the potential of harm against Canada's critical infrastructure as well as the legal avenues that are available to counteract them while also respecting the rule of law. An example of this includes expert witness Lieutenant-General Michael Day' opening remarks (42nd Parliament, 2018):

> With regard to electronic surveillance and security, I admit to an incredulity at either the inability or naïveté of Canadians in general, and quite frankly, the government in particular, accepting that there must be rules and policies surrounding these activities. It has shocked me. Over the last four or five years, I've worked a lot in the cyber domain. It's shocking to me how little effect successive governments have had in addressing the cyber-threats that this country faces on a daily basis. The vulnerability of our energy grid, the financial sector, among others, and the lack of a governmentwide set of policies and legislation to enforce compliance leads me to believe that we are living in a country that is now fully compromised by foreign actors at the state and non-state level. (p. 2)

Whilst Mr. Day's comments here outline a digital threat landscape that has eluded appreciation by Canadians, in the same remarks he also detracts from the predominant narrative of other expert witnesses when examining the new mandates being granted to Canada's NSA's and concerns of disproportionate empowerment (West, 2018; Nesbitt & West, 2019). His remarks further denote the existence of a normalization by Canadians when it comes to appreciating the surveillance threats the cyber domain has and how previous government responses to addressing these vulnerabilities is lacking. In seemingly direct opposition to Forcese and Roach's (2015) prior analysis of metadata collection and bulk surveillance of Bill C-51 and its eroding effect towards privacy, Day asserts that (42nd Parliament, 2018):

> The CSE legal mandate is a good and useful step, but it's only part of the picture. I am a strong believer that mass surveillance metadata, not individual surveillance or collecting

> individual information, and the power of directed and non-directed machine learning are critical to embrace and to better understand the space in which we are working. (p.2)

Again, we can observe here that Day's testimony largely represents a shift in narrative of the concerns raised by most scholarly research that preceded C-59's deliberations that focused on the expansion of and codifying of CSIS and CSE's mandates to account for bulk surveillance via the acquisition and analysis of both foreign and domestic databases (Nesbitt & West, 2019; Nesbitt, 2020; Parsons, Gill, Israel, Robinson, & Deibert, 2017).

Further examples of normalizations were also present when examining the threats that foreign governments, notably China and Russia, have on the Canadian populace via disinformation campaigns through social media. Speaking on this concern, Honorable Harjit Sajjan, then Minister of National Defence, explains (Standing Committee on Public Safety and National Security, 2018):

> My bigger concern, I'll be honest with you, with nations like Russia, is how they can take cyber and what we call hybrid warfare, such as with what's happening in Ukraine, and try to manipulate and influence populations. That is a concern and not just strictly from a government perspective. We have to make sure we educate our citizens and our media. (p. 9)

This comment referring to Russia's relatively newfound use of social media for conducting disinformation campaigns aligns with Buchanan's (2020) discussion on the 'organic reach' that these campaigns have when it comes to utilizing social media algorithms and exploiting individuals who may be less competent in digital media literacy to detect disinformation in such a way to disseminate disinformation on a national scale. These concerns of normalized unconventional methods in fifth-dimensional warfare were also echoed by Raymond Boisvert during his testimony concerning the need of ‘modernizing’ CSE’s mandates through C-59 when he also notes that enemy states “noted the ease and the immediate benefits of undermining our democratic processes by undermining people’s trust in institutions, as well as our ability to conduct respectful and constructive dialogue” (42nd Parliament, 2018, p. 11). These two examples of testimonies made by expert witness’s help illustrate how the committee holds the view that that Canadians have become normalized to disinformation online without resources to help discern the credibility of their sources. Between mass media coverage, social media exhaustion, and the surreptitious nature of how these attacks leverage commonly used networks, Canadians have become accustomed to disinformation, but not immune to it.

Contained in both Hajjan and Boisvert’s testimony we can make 2 distinct findings relative to normalization. First, these testimonial accounts reflect a growing concern of the hijacking of traditional social media platforms to spread disinformation amongst a population that has become a new method to conducting sabotage and influence offline violence (Bradshaw & Howard, 2018). Furthermore, it can also be observed that a normalized trust of social media platforms and IoT devices exists despite knowledge of how they create pathways to data harvesting and exploitation. Secondly, Hajjan’s remarks to the need of properly educating citizens and media reflect the potential of affirming initial research conducted by Arayankalam and Krishnan (2021) that examined how social media disinformation online can adversely impact citizens via Agenda-Building Theory. Finally, these findings help to support the occurrence of microdeviations by providing qualitative evidence specifically towards how disinformation campaigns online and the naivety of Canadians in understanding the complexities of vulnerabilities in the cyber domain as it relates to surveillance or data harvesting can be reflective of normalizations made towards them.

Theme 2: Moral Panics

For the second component of Microdeviation Theory, moral panics informed by a “manufactured uncertainty” towards digital technologies must be present as they inform the perspectives that lawmakers may have towards perceived digital threats. Popham (2018) notes that these anxieties regarding digital technology are effectively “products of modernization” that are informed by “digital futures” (effectively the risks perceived of contemporary technology and beyond that can be informed by depictions in fictional media) and become at risk of growing out of legislative control or outpaced by the oftentimes slow legislative process (p. 163). This generally occurs when such normalized deviancies progress past the point of containment either through public outcry or corporate dictates. Furthermore, microdeviation theory proposes that these moral panics may be seized upon by legislative bodies to depict the entirety of technology or the internet as that of being a lawless entity in need of far-reaching oversights.

However, an unanticipated finding of this research concerns the branching of narratives reflective of these moral panics into 3 distinct themes. Rather than narratives only focusing on anxieties of contemporary technology, testimonial accounts were found to be representative of fears concerning the digital advancement in terrorist or foreign states, foreign espionage tactics augmented by technology, and generalized fears concerning a growing legislative divide between what is captured in national security legislation and what technologies currently or theoretically exist that can outpace it (hereby referred to as “Internet Futures”). Of these 3 sub-themes, evidence of themes reflective to digital advancement in terrorist/foreign groups were captured 47 times, with testimony concerning foreign espionage capabilities occurring 26 times, and instances of internet futures occurring in 75 instances. Additionally, while the findings on these sub-themes will demonstrate this, it's important to note here that a common trait persistent in all 3 was that of a need to "modernize" Canada's NSA capabilities to dealing with threats in a digitalized threat environment.

The first sub theme, digital advancement in terrorist and foreign actors, emerged from testimony focusing on the utilization of contemporary technologies. This included references to how modern terrorist groups including Daesh have increasingly used traditional social media channels to disseminate propaganda and recruit followers for radicalization. Drawing on sources provided by both CSE (2019) and CSIS (2018) publications of threats facing Canada, this included examining testimony on internet-based disruption campaigns, as well as the "fifth-dimension" of warfare pertaining to global digital conflicts. These deliberations materialize when examining testimony focusing on Canada's national security against an expanding digitalized threat environment. For example, Dr. Christian Leuprecht appearing on behalf of the Department of Political Science of the Royal Military College of Canada remarks in his testimony that (Standing Committee on Public Safety and National Security, 2017):

> The fundamental conditions have changed. The security threats and vectors are much broader and much deeper than they have ever been. If you think about hypersonic manoeuvrable cruise missiles, intercontinental ballistic missiles, cyberspace, violent extremism, terrorism ideology, and also matters such as the globalization of organized crime, these are all things that we can't just keep away from our borders. They affect us here now, and they affect us every day. The security environment has fundamentally changed. The premise that we're somehow safe because we're far away from the troubles in the world simply no longer applies. (p. 10)

Here, we can observe that Dr. Leuprecht's testimony alludes to how contemporary technology has drastically changed the threat landscape so much so that traditional borders to conducting warfare can become obsolete as international groups weaponize the internet to conduct attacks on Canada's critical information structures. We can also observe here that the qualifications of Dr. Leuprecht help to give considerable authority to his observations surrounding manufactured uncertainty towards future threats by acting as a moral gatekeeper and use generalized terminology that can further incite anxieties surrounding the internet and other forms of technology.

Another finding surrounding the growing use of technology in national security cases concerns the use of encryption protocols and their hindering effect on conducting investigations. In the case of C-59, this includes cases whereby terrorist groups such as Daesh or domestic right-wing terrorist groups incorporate social media as an avenue to recruiting possible members for further radicalization via encrypted channels such as the Dark Web or the use of sophisticated encryption software to mask communications from being intercepted. The exchange between committee member Pam Damoff and Deputy Chief Constable Laurence Rankin of the Vancouver Police Department provides an illustrative example of how encryption can hinder the progress of investigations (Standing Committee on Public Safety and National Security, 2018):

> Ms. Pam Damoff: I just want to start by thanking you both for your service and for being here today with your testimony. It's much appreciated. I first want to start on the encryption piece because when we were doing our study on the national security framework, the chiefs of police were here talking about the need to have access to encrypted data. Then when we subsequently went on the road with the committee across Canada and had further witnesses, we heard overwhelming testimony that encryption isn't

> what we used to think about during the First World War or Second World War where it's encrypted data and somebody breaks the code and everything's good. It's actually when we give a back door to the good guys, like you folks, we actually are giving a back door to the bad guys as well. I've had numerous conversations with people who work in that field who said that's absolutely true. You're in a bit of a conundrum here, as you don't want to make it easier for the bad guys to have access to data. I'm just wondering if you want to comment on that and if there's anything in this legislation that would be able to assist you without also assisting the bad guys from getting access to data. Either of you would be fine.
>
> D/Chief Laurence Rankin: I'll start. I don't know if there is an easy answer to that question. I'd say that the barrier of encryption prevents us from obtaining a full picture of the evidence that is in the possession of the individual the police are investigating. I've talked to some of my tech crime people and they say you can have encryption technology today that will eventually be defeated and there will be a workaround or, though research, we'll be able to find a way, if you will a back-door way, to defeat the encryption. I think that whatever we will come up with, the bad guys will find a way or discover it in the same manner. I think what we find now is that police are simply not equipped to deal with it as effectively, in some cases, as the bad guys. That's the position we find ourselves in time and again. (p. 6)

The above exchange helps illustrate how contemporary and future technologies can provide a premise for situating the tipping point of the need for legislative changes. M.P. Damoff aptly notes that previous interpretations of what encompasses encryption is beyond what it used to be with regards to military intelligence in both World Wars, and that facilitating back-end encryption access for law enforcement can also inadvertently provide motivated criminals the same opportunity whether it be through that same back door or the creation of a new method. Rankin's testimony to that matter also contrasts with evidence of manufactured uncertainty as the prevalence of new technologies or encryption methods on an almost daily basis can easily disrupt or circumvent any attempt to combat encryption back doors being entrusted to law enforcement when conducting investigations.

When considering themes of internet futures, Popham (2018) notes that these elements of manufactured uncertainty must be present as they inform the perspective that current legislation cannot effectively meet the perceived impacts that further technological developments have. These anxieties can be driven not only by what contemporary technology is capable of but can "create as many uncertainties as they dispel" (pg. 163). As such, when considering evidence of internet futures, the concerns of modernizing or "future-proofing" C-59 was considerably evident. Regarding CSE's new mandates contained in C-59, Hon. Harjit Sajjan states that "However, what is needed now are modernized authorities to ensure that CSE is able to continue to adapt in this ever-changing environment both today and into the next 70 years." Regarding the new powers being granted to CSE to assist the Canadian Forces via cyberoperations, Sajjan further states that (Standing Committee on Public Safety and National Security, 2018):

> Third, and of particular interest to National Defence, the technical and operational-assistance aspect of CSE's mandate would clarify that CSE is allowed to provide assistance to the Canadian Armed Forces and the Department of National Defence. This will enable CSE to better support Canada's military missions and the brave women and men of the Canadian Armed Forces serving in theatre. Of course, CSE already provides important intelligence to the forces under the foreign intelligence aspects of CSE's

> mandate. This legislation would allow CSE to do more to help them to, among other things, conduct active cyber-operations in support of government-authorized military missions. Bill C-59 will enable CSE and the Canadian Armed Forces to better co-operate to ensure the best use of tools and capabilities to meet mission objectives. (p. 1)

Pairing this testimony with Hon. Harjjan's previous comments towards modernizing Canada's NSA mandates, 2 specific findings towards both information sharing amongst agencies and modernization tropes can be examined. First, while Maras' (2017) research examining intelligence sharing amongst agencies considered U.S. counterparts, the underlying premise to Hajjan's testimony here appear to indicate that a similar proposition is being made that the integration of CSE's cyberoperations will do more to bolster CAF military operations. Second, the initial remarks towards the further modernization of Canada's national security strategies to account for decades of technological change also support microdeviation theory by providing possible narratives towards manufactured uncertainty. The reframing of CSE's mandate proposed by C-59 towards facilitating a more active role in military operations harkens back to West's (2018) initial remarks on considering the potential consequences that cyberoperations have towards foreign sovereign states that will inevitably be breached.

Finally, discussions around the capabilities of foreign entities conducting cyber espionage or sabotage were a prevalent theme when considering narratives structured around moral panics. Important to note here is that while this third theme may seem semantically similar to digital advancement in terrorist groups, a key difference notes that these excerpts solely focused on the manufactured uncertainties towards the capabilities of foreign state actors specifically. Preceding Hon. Sajjan's comments surrounding Russian capabilities to conducting hybrid warfare that was demonstrated as a normalization example, he further integrates C-59's perspective of cybersecurity in the overall threat environment (Standing Committee on Public Safety and National Security, 2018):

> In the overall context, we have to look at current threats, threats that are potentially emerging, and what we can predict as future threats. This is the responsibility of the government, to make sure that we have the right resources to be able to deal with threats today and tomorrow. We've been dealing with non-state actors for some time, as well as with state actors. Cyber is a significant concern, but I also want to say that, because we have done extremely well in Canada, CSE has the ability, the expertise, to give Canadians the assurance of tremendous safety when it comes to cyber. However, as you know, with technology, we need to stay at the cutting edge. (p. 9)

Taken into the context of the modernization push that preceded C-59's introduction, Hon. Sajjan's testimony here highlights the threats that foreign actors have regarding their expansive capabilities to conduct acts of aggression against Canada when leveraging IoT technology and the internet. However, it also becomes apparent here just how pervasive the terms "cutting edge" and "modernize" are integrated through this testimony to portray possible threats that currently cannot be comprehended or mitigated.

Theme 3: Disproportionate Legislative Responses

Following the occurrence of the previous two premises to Microdeviations, the third element of the theory calls for critical consideration of the resulting legislative responses that are formulated to control or mitigate harms from technology. Considering the human elements behind the technology being used, Popham (2018) notes that the prevailing narrative amongst legislators is that they must also be vulnerable to human intervention. Revisiting the example regarding the DMCA, which sought to control supposed rampant piracy of media online, many scholars have long argued that the act was the product of oversight in legislative responses that gave disproportionate powers to media companies that own the property in controlling media-use online that fails to address the underlying causes to piracy online (Patry, 2009). As such, this premise was utilized when considering examples of C-59's mandates that may provide evidence to whether C-59 was playing upon perceived risks of internet futures or normalizations of deviant elements of the internet and technology with its drafting of powers towards Canada's national security.

To begin, the findings on this matter of microdeviation are best supported by the following exchange regarding C-59's overtly vague definition of electronic datasets and what this means towards Canada's NSA operations (Standing Committee on Public Safety and National Security, 2017):

> Ms. Julie Dabrusin: Thank you. Professor Forcese, when you were talking about datasets, I had a couple of questions. First of all, do you find that the definition for "dataset" in part 4 is sufficient?
>
> Prof. Craig Forcese: Datasets are not robustly defined, so the definition of "dataset" is fairly open-ended. It's an electronic record characterized by a common subject manner, without further resolution as to what that means. Left with a vague definition, I turn instantly to what checks would exist to rein in an egregious, overbroad understanding of what a dataset might be, as compared, say, to the Security of Canada Information Sharing Act, where I agree with what was said before: that concept is overbroad as well. (p. 15)

This statement is demonstrative of concerns that portions of C-59 extended beyond practicable definitions and instead offered wide conceptual definitions. As Forcese explains above, these oversights on providing definitions to datasets in such a way carries the possibility of being subject to wider interpretations and possible exploitation. At issue here is whether the threat of having innocent Canadians broadly defined publicly available data subjected to C-59's information sharing protocols and exploitation warrants the inclusion of a broad definition. Similar concerns relative to the inclusion of Canadian metadata in Canada's NSA mandates in Bill C-51 were also raised by Forcese and Roach (2015) when considering how even anonymous datapoints including call locations, cellular tower proximity, and dialogue length could still provide intimately identifying data about an individual alongside "big data" which includes the amalgamation and exploitation of smaller datasets for the purposes of conducting intelligence operations. Ms. Lex Gill, of the National Security Program Canadian Civil Liberties Association, echoes these concerns relative to the broader legislative definitions given in C-59's terminology. She notes that while CSE's mandates specifically bar the agency from conducting surveillance on Canadians, that the publicly available data clause to CSE operations in C-59 "exacerbates this privacy risk" via the creation of exceptions in the bill that facilitates "the collection of Canadian data, including one which allows its acquisition, use, analysis, retention, and disclosure, so long as it is publicly available" despite CSE assurance in C-59's meetings that this would not be the case (Standing Committee on Public Safety and National Security, 2017, p. 13). Her comments towards public data exceptions in C-59 argue that the accountability mechanisms, while a welcome change to review mechanisms, are effectively being undermined by broad definitional concepts and clauses.

On the opposite end of the public data debate, another important finding here considers Craig Forcese's cross examination on how to reign in the definition of publicly available datasets and the difficulties it will entail given the subject matter and the need for Canada's NSA's to be able to conduct their mandates without restrictive terminology (Standing Committee on Public Safety and National Security, 2017):

> Absent a specific suggestion in this bill, I don't know that I would single anything out as better embedded in regulation. Professor Wark and Professor Carvin this morning both mentioned that the concept of dataset is broadly clothed. If we were to define it rigidly in the act, then we may have a problem. However, we don't. We have an open-textured definition of "dataset" that's then subject to scrutiny by independent oversight entities. That's an example of flexibility. There's also the prospect of "exigent circumstances", which the bill recognizes in several instances. I don't see this as overly restrictive, and to a certain extent, I think a lot of these changes surface internal guidelines that the services have in fact employed. I think codifying it in legislation is actually important because it creates a sense that these are agencies that do comply with the rule of law that people are otherwise unaware of because these standards are opaque and buried in operational policies. I think that's important in terms of credibility. (p. 19)

It's here that we can observe that as Canada's NSAs require more latitude in accordance with their mandates, that a significant obstacle will be determining what aspects of digital datasets can be fully encapsulated via legislation and what other factors need to be given space to operate. This exception also raises concerns whether the maneuverability given to Canada's NSA's can be properly kept in check via both the NSIRA and the Intelligence Commissioner. During his introductory remarks, Michael Day goes one step further with his own assertion that the restrictive components to electronic surveillance and cybersecurity mandates will hinder Canada's NSA's in combatting cyber-threats (Standing Committee on Public Safety and National Security, 2018):

> It seems to me that much of the public debate on the bill in question, C-59, is about legal mandates, compliance, oversight, and governance. I don't wish to imply that this isn't needed, let alone value added, but rather suggest that the necessity of this conversation should not be mistaken for sufficiency. By itself, the debate on those issues is insufficient. In a rapidly changing world, an equal amount of discussion should be given to the efficacy of the security and intelligence agencies and supporting departments, how well they work together, how rapidly they are able to, not just respond in the moment, but adjust to changing threats, etc. (p. 2)

Michael Day's testimony not only here but on other facets of C-59's national security strategy dichotomizes prevailing narratives and evidence of other expert witnesses that sought to integrate more concise restrictions to intelligence activities in the furtherance of each NSA's mandates. Tying this back towards Microdeviations, the remarks run counter towards any unanticipated effects that C-59 can have by arguing that considerations need to be given towards the efficacy of Canada's own agencies against a rapidly changing threat environment. Furthermore, the remarks here also go against initial analysis of C-59 as conducted by Parsons et al. (2017) and Nesbitt and West (2019) that suggests codifying mass-surveillance as authorized intelligence gathering can have drastic implications towards egregious and unmitigated forms of unselected mass surveillance.

While a section examining findings on C-59's addition of active and defensive cyberoperations to CSE's will occur in the second half of this chapter, it's important to demonstrate here the initial findings on cyberoperations specifically when examined in the Microdeviation context. Most notably, the inclusion of cyberoperations to CSE's mandate was found to often be viewed as one of the more disproportionate factors of C-59 given its novelty in addressing cyberthreats internationally (Parsons, Gill, Israel, Robinson, & Deibert, 2017; Nesbitt & West, 2019; West, 2018). In her opening remarks, executive director of OpenMedia, Ms. Laura Tribe, considers the addition of cyberoperations as being (Standing Committee on Public Safety and National Security, 2018):

> The new active and defensive cyber-operations powers proposed in Bill C-59 for CSE are directly opposed to the wishes of the majority of Canadians. We asked for privacy, but instead we got an out-of-control spy agency with even more extreme powers than before. Security and privacy experts throughout Canada have expressed in great detail the issues with the proposed bill and the changes that need to be made to protect the privacy and security of Canadians. Experts have warned of the consequences of granting powers like these, powers that will be all the more dangerous given the lack of adequate oversight included in the bill. (p. 2)

Laura Tribe's comments here help to illustrate the backdrop that the new active and defensive cyberoperation mandates have when considering Microdeviation integration. These findings further help explain the hesitancy to expanding the powers of Canada's NSA's, specifically CSE, when it comes to being a more active in Canada's national security strategies. Notably, her comments further reflect existing research by West (2018) that considers the addition of the two mandates as being the equivalent of mandating state-sponsored cyber-attacks.

Microdeviations Findings: Conclusion

Given the demonstration of initial findings above, it can be observed that the tenets of Microdeviation Theory can aid in the examination of legislative responses to digital threats, as were apparent in C-59's initial drafting and deliberations on the expansion of NSA mandates. Given that the primary objective of this thesis was to examine the narratives employed by committee members and expert witnesses alike for potential applications of the concept, it's important to note here that there was a significant amount of testimony contained in C-59's meetings that was representative of the 3 core elements needed to justify its inclusion. Of the 520 codified excerpts of testimony, 219 instances were captured that supported tenets of Microdeviation.

General observations of the dataset seem to indicate that Canadian naivety to digital privacy, disinformation, and the willingness to impart seemingly banal types of data online for the public eye informed most of the discussion of normalization to the objective reality of the digital era. As illustrated above, this included references to how Canadians increasingly use a variety of different technological products and software that become sources of data harvesting or are readily accessible to the public. To use some of these products, they increasingly require the consent of the user to have access to certain forms of data (including location, contacts, and other admin privileges) which is willingly given less they be barred from future usage. Further, the meetings saw substantial debate surrounding the digital capabilities of foreign states and individuals to leverage online social spaces and global interconnectedness in such a way to conduct sabotage or web revision. At face value, these narratives seemingly harkened to a new "digital cold war" and a need to develop a "futureproofed" national security legislation equipped with new and novel powers to protect Canada's national security interests both domestically and abroad.

FINDINGS V1.2

Findings V1.2: External Emergent Themes

Before concluding the initial findings, it's important to also note the external themes that became prevalent during this study to warrant their inclusion in the forthcoming analysis. While this study initially approached data collection contingent on the 3 overarching themes to Microdeviation Theory, Saldana's (2014) QDA methodology also facilitated the generation of new codes via inductive reasoning and constant review and revision of emergent themes contained in the data that could supplement a projects analysis. While examining the evidence contained in C-59's legislative process, four themes outside of Microdeviation Theory were identified that had qualitative significance to the implications of this projects analysis. This includes references to themes of how C-59's mandates can impact Canadian charter rights and Canadians digital privacy online (146 references), descriptive terms used by the committee to describe facets of the internet and cyberconflict (39 references), evaluations of C-59's new NSA review agency (NSIRA) (51 references), and most importantly, the discussions surrounding C-59's cyberoperations mandate for CSE and the possibility of entering a cyber cold war (65 references). This section of the findings chapter will aim to give a brief overview of these themes alongside their Microdeviation counterpart.

Theme 1: Charter Rights & Digital Privacy

To begin, themes relevant to concerns of Charter protections to privacy of Canadians in a digital age were amongst the most prevalent identified outside the 3 themes related to Microdeviation. For the purpose of this study, examples of this theme considered evidence discussing C-59's role in a digital age and how certain mandates contained in the bill can be related to reasonable expectations of privacy as interpreted by section 8 of the Canadian Charter.

Furthermore, evidence of these themes was also captured when discussions surrounding matters of Canadian metadata online as explained previously by Forcese & Roach (2015) were concerned. The premise of metadata's role in privacy debates against national security legislation here is not entirely new. Both Forcese and Roach (2015) noted in their analysis of Canada's previous national security legislation C-51 that the utilization of metadata towards national security mandates can pose dire implications to Canadians privacy interests despite having certain exemptions, specifically with CSE's then mandate to not conduct surveillance operations at Canadians either at home or abroad. Congruent with the findings here in C-59 is the concern that the "breadcrumb" nature of metadata online doesn't go far enough to protect Canadian interests of privacy as the elements that makeup metadata (namely approximate geographical location to cell phone towers, call length, or other attributable data) can be triangulated alongside other minor data-sources in what Forcese and Roach refer to as "big data."

Over the course of gathering data, it was noted that these concerns to digital privacy in an advanced age permeated discussions surrounding both themes of normalizations in digital subcultures as well as themes highlighting potential disproportionate costs to C-59's mandates; most notably being the impact that mandating cyberoperations in CSE's legislation can have towards Canadians publicly available data contained in Part 3 subsection 24(1) in the bill. Regarding the potential naivety of Canadians to their public profiles online, committee member Mathew Dubé notes "the argument can be made that it's publicly available information and that's too bad for people who maybe don't manage their social media very well", and it's the interaction illustrated here between Charter rights and how social media platforms afford an avenue to forgoing privacy interests becomes apparent (Standing Committee on Public Safety and National Security, 2017, p. 5). This finding can also be supplemental when considering

Microdeviation as it relates to disproportionate legislative responses as privacy becomes more of a commodity that diminishes unless the user actively takes steps to protect their data online. The exchange between committee member M.P. Julie Dabrusin and Honorable Jean-Pierra Plouffe, previously the commissioner of the CSE which oversaw their activities prior to the introduction of the NSIRA, further illustrates these concerns (Standing Committee on Public Safety and National Security, 2018):

> They suggest that there are no charter or privacy rights that would be affected by these techniques that will be used outside of Canada. This is with regard to the CSE. Unfortunately, I don't necessarily agree with that view, and neither does the Department of Justice, which is the legal adviser to the government. I'm quoting from the justice department's legal opinion, page 9 of a document entitled “Charter Statement - Bill C-59”. It's short, but it explains my position. I quote: The provisions authorizing active cyber operations would not by definition engage any Charter rights or freedoms. However, specific activities authorized under this scheme could potentially engage rights or freedoms. The considerations that support the consistency of this aspect of the mandate with the Charter are very similar to those supporting the consistency of the defensive cyber operations mandate. One difference is the distinct purpose of active cyber operations, which would be to further the government’s compelling objectives in relation to Canada’s international affairs, defence or security. (p. 3)

The above exchange helps to further illustrate how considerations need to be given when asking what limitations, if any, need to be examined when granting powers such as cyberoperations especially as it relates to Charter limitations. Although the wording of C-59 requires authorization on certain active and defensive cyberoperations, Plouffe’s testimony helps to highlight how certain activities that are integrated post-authorization can likely trigger them but will not require re-approval.

Forcese further expands on the complexity of only protecting Canadian data from foreign intelligence operations during his meeting for C-59 when he notes that the authorization process is only triggered when they circumvent acts of Parliament and do not have a trigger for the same protections outside of this scenario. He further argues that some of the intelligence gathering activities of Canada’s NSAs can trigger reasonable expectations of privacy while not violating an act of Parliament. Regarding how metadata collection avoids this violation, he notes that the solution would be to expand this trigger to include (Standing Committee on Public Safety and National Security, 2017):

> The new system will only resolve the constitutional problem if it steers all collection activities implicating constitutionally protected information into the new authorization process. The problem is this. Bill C-59's present drafting only triggers this authorization process where an act of Parliament would otherwise be contravened. This is a constitutionally under-inclusive trigger. Some collection of information in which a Canadian has a constitutional interest does not violate an act of Parliament, for example, some sorts of metadata. (p. 1)

The finding here is notable primarily as it reflects Austin’s (2012) analysis of how the rule of law, in the face of growing surveillance technology, has subtly narrowed the legal definition of privacy to facilitate the expansion of state authority powers. The deliberate codifying of only requiring authorization when an act of parliament is triggered further expands the scope of what encapsulates surveillance whilst disregarding the possibility of individual stakes in privacy.

Theme 2: Situating Canada's responses in a global context

Throughout the process of data collection, it became apparent that various committee members and expert witnesses would often engage in matters focusing on descriptors indicative of modern internet subcultures, as well as putting fourth suggestions of the growing integration of cyberconflict in contemporary battlefronts. Additionally, there was a growing narrative that sought to compare the cybersecurity efforts of Canada's own national security legislation towards that of other foreign states typically included in the Five Eyes alliance. Effectively, this theme was generated in order to capture these instances as they contained dialogue that provided underlying perspectives of committee members and expert witnesses alike as to how C-59 be constructed to properly reflect contemporary technology and be of sound standing when compared to other allies internationally.

These types of narratives were utilized to describe how foreign nation states both friendly and antagonistic had rapidly cultivated their own states to be more proficient with the development of new and novel methods of cyberwarfare technology and how Canada itself needs to bolster their own defensive strategies with haste. A notable example of this concerns Mr. Raymond Boisvert's opening remarks during the January 30th meeting where he remarks that "offensive cyber-tactics have been developed and are being applied by the best private security firms in the world", and notes that vital energy system attacks such as from cases involving Ukraine and Germany warrant the need to empower CSE to carry out its mandates to protect Canada from any potential attack on its own infrastructure (Standing Committee on Public Safety and National Security, 2018, p. 11).

Additionally, Canada's own national security mandates were often compared to those of other allied states in the Five Eyes Agreement, as this partnership facilitates the exchange of intelligence amongst member states for the purpose of carrying out the protection of their own borders against threats (Roach & Forcese, 2015). A notable inclusion of this concerns the integration of CSE's mandates to facilitate the agencies own resources alongside the Canadian Armed Forces for the purpose of augmenting traditional military operations with the supplemental authority of CSE intelligence. Speaking to the committee, Hon. Harjit Sajjan notes that this integration "puts us in line also with our Five Eyes partners" and expresses that he was surprised to see that CSE hadn't been given this legislative power in other previous national security legislation as it would allow the Canadian military the ability to leverage the agencies technical expertise (Standing Committee on Public Safety and National Security, 2018, p. 1). Speaking in a previous meeting, Professor Stephanie Carvin is also supportive of the need to integrate CSE into a more active cyber-role noting that in comparison to other Five Eyes allies "many of whom have been quietly encouraging Canada to enhance its cyber-presence in the wake of cyber-threats from North Korea, China, and Russia". She further notes here that while the legal and ethical challenges need to be appreciated, that by integrating these new powers on statutory footing we demonstrate to our Five Eyes allies that while NSA operations become more transparent (referring to NSIRA review), we also situate Canada as "a more reliable, dependable partner" (Standing Committee on Public Safety and National Security, 2017, p. 6).

Theme 3: Cyberoperations and the Cyber Cold War

As mentioned above, C-59 was often touted during testimony as a modernizing legislation that aimed to bring Canada's NSA's and their respective mandates to a point where their powers would effectively become "futureproof" for the foreseeable future. Prior to the enactment of C-59 however, the CSE had not yet been formally established as a proper national defence agency, rather, their mandates were contained in Canada's *National Defence Act (2001)* and operated within the Department of Defence (Nesbitt & West, 2019). This all effectively changed with C-59's enactment as it formally established the agency as a separate entity governed by the National Security Intelligence Review Agency and saw their mandates expanded to better account for international threats and cybersecurity assurance. However, this expansion saw the CSE's 3 mandates expanded to 5, adding both active and defensive cyberoperations to protect Canada's information infrastructure and empower the agency to be more proactive in countering threats abroad. Regarding CSE, these 2 mandates were amongst the primary area of concern for the committee as the new powers were effectively new and hadn't been integrated before. Furthermore, external academic inquiry such as West's (2018) analysis on the potential implications towards international treaties posed questions to whether these new powers could lead to inadvertent acts of war on other sovereign states. Additionally, initial findings relevant to C-59's new mandates also indicated a growing concern amongst committee members and expert witnesses alike concerning the rapidly evolving "cyber-arms race" harkening back to fears of a second Cold War, this time concerning the seemingly out of control development of new and novel technology that could see warfare branching into the fifth dimension.

Regarding cyberoperations, initial lines of questioning during C-59's debates centred on identifying and potentially getting ahead of concerns relevant to whether the utilization of cyberoperations for Canada's national security was disproportionate to the tangible benefits they would provide. Speaking on how cyberoperations could protect critical infrastructure or prevent possible cyberattacks, then Chief of CSE Greta Bossenmaier notes that (Standing Committee on Public Safety and National Security, 2017):

> Some of the proposals in the legislation that's in front of this committee would allow us to further use our cyber-capabilities to better protect Canadians' information. I mentioned one already, in terms of being able to protect and deploy our systems on nongovernment systems upon the request of a critical infrastructure owner, for example. The minister referenced another one where we would be able to actually go out and try to prevent an attack against Canada or Canadians or Canadian infrastructure before it happened. These are two examples of how this act would help us better protect Canadians. (p. 17)

During the same meeting, Hon. Ralph Goodale further testifies that the measures being proposed for Canada's NSA's prevent agencies from having to "sit back and wait to be attacked, even though you know it's going to happen". Hon. Harjit S. Sajjan further echoes these remarks noting that C-59 will empower CSE to become a more proactive agency in conducting their foreign intelligence mandates as well as becoming more empowered to work within non-federal critical infrastructure to secure Canadians from external cyberthreats. As mentioned before in this study's findings surrounding disproportionate legislative responses however, this further empowering of CSE to conduct such cyberoperations carries with it the potential for considerable blowback on an international scale that should not be disregarded.

Testimonial accounts linked to discussions surrounding cyberoperations also carried with it narratives that envision the evolving digital landscape as a new threat environment reminiscent of the Cold War. The expansion of CSE's mandate to include the capability to conduct cyberoperations and the unknown nature of what they will include in practice was a cause for great concern amongst expert witnesses. Given the extreme capabilities that cyber-attacks can have in terms of inflicting serious impacts on most of Canada's critical infrastructures, evidence that focused on a coming "Cyber Cold War" was especially prevalent, as the exchange between committee member M.P. Peter Fragiskatos and Scott Newark, a former special security advisor on counterterrorism, illustrates (Standing Committee on Public Safety and National Security, 2018):

> Mr. Peter Fragiskatos (London North Centre, Lib.): I take your point that in new threat environments, Canada and other democracies need to really adapt. You're familiar, I think, with the Centre for International Governance Innovation in Waterloo. They recently published a piece, and I want to read a quote from it and get both your thoughts. They say, as follows: ...if the Cold War taught us anything, it is that sometimes the best way to ensure that everyone lives in peace is to ensure that everyone has the ability to destroy one another, otherwise known as the doctrine of mutually assured destruction. Cyberweapons that have clear offensive uses do just that. They show the world (or at least those that know you have them) that should you be attacked, you can escalate and retaliate in turn. Is this an apt way of looking at where we find ourselves today in terms of international security?
>
> Mr. Scott Newark: First of all, I think it's important to appreciate that the acronym for mutually assured destruction is MAD, but part of the complexity in that is that the threats are not necessarily from state actors. That's a challenge in itself. The thing that concerns me the most, frankly, is advanced persistent threats. They're already planted and they're sitting there waiting for the folks in Pyongyang or Beijing to decide that now is the time we're going to do this. Having said that, however, I think it is critically important, given the authority and the power that's there and its ramifications, that this should not simply be one branch of government reporting to another, then signing off and saying that's it. I think this is something, given its importance, that requires some form of independent

> review and authorization. Although we would want all of these circumstances to be considered exigent, some kind of a review should be done after the fact. I think, just as a general principle, that unless there's a reason not to have that independent oversight, the nature of the authority is such that it requires that balancing effect. (p. 4)

The above exchange helps to illustrate how the spectre of a growing cyber arms race is framed and presented as a call to arms in terms of increasingly expanding Canada's offensive capabilities in the cyber realm. As this study also found in terms of findings relating to previous instances of manufactured uncertainty, the internet has increasingly become a new front in terms of international conflicts that requires the passing of legislation such as C-59 to protect Canada's infrastructures pre-emptively rather than reactionary.

DISCUSSION

i. Introduction

This thesis endeavored to provide a critical examination of the narratives and evidence both committee members and expert witnesses utilized to advance certain policy positions or legislative concerns to the powers being granted in C-59 towards Canada's national security agencies. I sought to explore committee dialogue – which ultimately shaped the nature of the CSE act – through the microdeviation lens, focussing on participants' use of narratives of manufactured uncertainty towards technology and rapidly evolving digital threats to national security to advance some of the more disproportionate or novel mandates based on the guise of modernizing Canada's national security strategies and legislation. Furthermore, I also sought to provide a commentary on how C-59's mandates could inform scholarly discussions in Criminology surrounding technosocial elements as discussed by Brown's (2006) *Criminology of Hybrids* by examining narratives and evidence in C-59's deliberations for perspectives relating to how technology and the internet has further augmented the capabilities of foreign states and individuals and the implications it has towards scholarly debates surrounding traditional cybercrime literature. The final objective of this research sought to examine how the underlying narratives to modernizing Canada's national security agencies and legislation via empowerment and expansion of their mandates towards a rapidly evolving digitalized society could withstand Charter constraints or violations.

The implementation of microdeviations towards Canada's national security policies proposes a new perspective in scholarly circles when considering digital deviance and IoT technology and how the two are increasingly becoming ingrained with one-another (Maras, 2015). The findings demonstrated in this thesis help advance key arguments made in Popham's

(2018) initial article while also expanding on Brown's (2006) conceptualization of the "criminology of hybrids" and how both the physical and digital elements of an individual are increasingly becoming resistant to classical criminological theories of crime that examine the two as separate entities. That is to say, the presence of microdeviations in C-59 carries implications towards traditional criminology and policy development that proposes physical or classical interventions to control cyber-criminal behaviour. Namely, the reality exists that individuals no longer visualize technology as mere tools to conducting criminal acts, but rather the proliferation of IoT technology and social media has enabled individuals to adapt them as extensions of their own bodies. As such, legislative attempts that focus on the multitude of fronts that the digital realm represents need to be able to appreciate how certain powers being granted towards the perpetuation of a more active surveillance or disruption can disproportionately harm innocent users especially in the context of withstanding human rights challenges. As Lyons (2015) noted in the wake of the Snowden revelations, the expansion of surveillance from individuals to mass surveillance can itself carry vast implications of potentially entangling innocent users in its web. This is not to say that the objective of this research was to paint C-59's policy goals in a bleak perspective, rather, the incorporation of the theoretical perspectives sought to provide a unique perspective in asking whether said policy objectives are appropriate and based on existing evidence.

This research was carried out utilizing qualitative methodology, most notably Qualitative Data Analysis via Saldaña (2014) as it allowed the constant revisiting and revising of the most prominent themes contained within the dataset while also initially approaching the dataset with pre-determined themes reflective of microdeviations. This meant that as research progressed, certain themes could be generated, merged, or discarded depending on qualitative value to the overall research project and facilitated the generating of preliminary analytical memos indicative of possible answers to the initial questions being asked. Initial results were promising as the testimonial accounts and evidence presented in C-59's deliberations aligned well with the deductive themes of microdeviations while also generating additional themes via inductive analysis that were supportive of the possibility of Microdeviation Theory's utility in examining Canada's national security legislation. Furthermore, the additional themes that were generated via QDA also provided additional points of analysis towards the implications that C-59 has towards the global onset of rapidly developing and leveraging of technology and the internet to a potential cyber cold war.

Discussion: Normalization of Digital Deviance

When examining the meetings for evidence of normalization, what became apparent at an early stage of this research considers how testimonial accounts and cross-examinations by committee members perceived global advancements in technology and the internet towards the balance of preserving Canada's national security. Notably, the prevalence of social media, smart home technology, and a perceived naivety from Canadians towards terrorist capabilities both foreign and domestic formulated what normalizations occurred in the context of what C-59 aimed to confront. Oftentimes it became apparent that some committee members and experts felt Canadians would typically forgo privacy protection online by virtue of the technology utilized in day-to-day happenings. For example, the prevalence of modern smart phones and other smart technologies integrated via the IoT across Canada have situated internet technologies as a central figure in most Canadians' lives. This new reality is reflective of Maras' (2015) arguments about the expansive role IoT technology has in a user's social life despite known risks. These forms of technology often come with an underlying cost in the form of data aggregates that can be used to measure user habits or individual predictability which in turn affects how private users can feasibly be free from surveillance (Maras, 2015). Furthermore, the growing market of IoT technology can also open users to malicious cyber-attacks that can leverage exploits or vulnerabilities which can easily spread to other connected devices nationwide. As was observed in these committee meetings, Canadians have been situated as users that have normalized or may not appreciate these costs by virtue of their continued usage despite the possibility of having their data possibly swept up in surveillance nets or be subject to cyber-attacks.

As demonstrated by questions posed by committee members to expert witnesses, the addition of the “publicly available data” clause to data available to Canada’s NSAs at face value appears to be a boon to conducting investigations as users will continue to freely share their daily lives online. The logical connection of this thesis’ findings concerns how similar narratives were utilized by both committee members and expert witnesses alike to demonstrate how Canadians have normalized these platforms that maintain public databases despite their potential to be included in surveillance activities or subject to exploitation. Similar to Forcese and Roach’s (2015) comments surrounding the controversial use of metadata against Section 8 privacy interests, both metadata and the broad definitions given to publicly available data for C-59 indicate that the discussion will likely continue for the foreseeable future on whether they need to be given reconsideration as technology users adapt devices ever more capable of collecting it. Furthermore, the integration of Microdeviation Theory to C-59’s meetings demonstrates that as technology and the internet continues to evolve and become more ingrained in user experiences that the normalization of trading privacy interests will become further commodified as a buy-in to its use; or as Maras (2015) notes, that the ability to retain anonymity will become increasingly more difficult for the development of IoT technology to reach its full potential. This effectively makes the negotiation of maintaining anonymity online a zero-sum game: that to continue using web-based services, you must forgo any personal stakes in maintaining anonymity and accept the possibility of having personal data shared online be subject to active surveillance by extension of the public data clause in C-59. In the wake of devices increasingly becoming connected to the internet and requiring frequent consent to data collection, this hypothetical becomes increasingly close to reality.

A final point regarding normalization that warrants revisiting here concerns the susceptibility of Canadians to disinformation campaigns online as well as findings from C-59's meetings that advanced concerns relative to the ongoing leveraging of IoT technology and the internet by foreign adversaries. (Arayankalam & Krishnan, 2021), the normalizations by Canadians towards the capabilities of foreign states or terrorist groups was framed in such a way that the potential impacts of deviance online were minimized or disregarded as being able to occur in Canada. Of interest to this study concerns how these normalizations were utilized by some expert witnesses and committee members as a vehicle towards some of the more disproportionate elements of C-59. Despite this naivety towards threats online, C-59 was oftentimes positioned as a needed response to better protect Canadians from threats that they may or may not be able to fully appreciate despite concerns of disproportionate abuse raised by other expert witnesses.

Overall, the framing of normalizations towards deviant elements of online subcultures and the progression of technology raises concerns of how typical users in Canada overlook them in their own daily usage. Despite their propensity of effectively being mass data aggregators of personal data, Canadians are continuously conceding ground on what constitutes private, personal data online. Whether by willful ignorance or lack of appreciation, the continued use of social media and software that increasingly requires new permissions to function means that Canadians will increasingly commodify certain elements of their own personal lives to maintain participation in digital communities despite vulnerabilities to exploitation. Furthermore, this was also observed when we consider the increasingly expansive ecosystem of SMART technologies that are being integrated into Canadian homes and businesses. These concerns were also echoed in certain testimonies that considered the advances being made in contemporary technology and national security when examining Canada's vulnerabilities to cyberattacks on critical infrastructure. As more devices are added to their networks, so too will the attack surface expand resulting in additional avenues to cyberthreats.

Discussion: Moral Panics and Manufactured Uncertainty

Across many of the meetings that took place, what became increasingly prevalent early on was how the need to "modernize" and "future proof" dominated most discussions surrounding C-59's refresh on national security objectives. For example, statements made by government officials suggest that they perceive social media and IoT technology as a growing threat to sovereignty, a domain that they see as having been leveraged by foreign state actors and domestic groups. Testimonial accounts by expert witnesses reflective of changing and adapting technology reflect anxieties about internet futures or manufactured uncertainty by employing examples of foreign adversarial use of developing technology such as AI and botnets to conducting acts of aggression through the internet.

Most notable in this study concerns the use of narratives and evidence to frame previous legislative responses in Canada against these perceived threats in the cyber-domain as being insufficient and unadaptable towards contemporary and future threat environments. Of the committee members and expert witnesses who generally expressed support for C-59, the bill was often touted as one that enables Canada to maintain its global competitiveness against evolving cyberthreats and codifying powers that would facilitate a stronger national security prerogative. A central concern reflective of the moral panic process in these meetings focuses on the apocryphal connection between online activities and vulnerabilities and major socio-political epochs like the cold war. The advancement and integration of contemporary technologies and internet subcultures including social media in these meetings were the main drivers used to further advance concerns that Canada's lagging legislative response was hindering the countries' efforts in the escalating cyber-arms race that foreign nations and terrorist groups were already involved in. These elements of fear were developed and used to advance concerns of normalized ignorance by Canadians towards these expanding vulnerabilities.

It is on this emergence surrounding findings that were reflective narratives reminiscent of cold war era fears that requires a great deal of consideration in terms of this studies implications. While the capabilities of motivated threat actors either domestically or abroad cannot be understated, oftentimes what this study found was those statements pertaining to how these attacks could be carried out digitally were often supplemented with evidence pointing towards the need to stockpile and expand powers that could be granted to Canada's NSA's. The use of these rhetoric's when advancing manufactured uncertainties was powerful in terms of providing the justifications needed for their inclusion in C-59. These forms of narratives were especially prevalent when considering testimony given by members of the then Liberal majority government such as Hon. Ralph Goodale and Hon. Harjit Sajjan. Like Graebner's (2000) analysis on the use of rhetoric to justifying U.S.A.'s stockpiling of nuclear weaponry, instances of these manufactured uncertainties towards the capabilities of fifth-dimension warfare permeated most of the discussions surrounding what forms of threats Canada faces in the near future and how a perceived lagging legislative response warranted the inclusion of new powers.

Discussion: Disproportionate Legislative Responses

The final arm of microdeviation holds that states will respond to inflated situations by developing disproportionate legal measures that do not adequately address contemporary digital threat environments. Popham (2018) argues that “public concern over an existing microdeviation can lie dormant until a catalyzing moment occurs at which point it is subjected to disproportionate response” (p.165). He further states that “these responses often take the form of overt methods of control as traditional authorities attempt to maintain their dominance over social space” (p.165). Most notable in this project concerns how evidence of this theme was reflective on both sides of discussion concerning the permissibility of these more extreme responses focusing on the expanded capabilities towards public data collection, broader codification of databases permitted in investigations, and most notably the addition of active and defensive cyberoperations. Whereas on one side these meetings contained testimony arguing that broad definitions and expanded powers were poorly defined or too exhaustive, the other side contained testimony advocating that being too restrictive on certain elements dealing in the cyber domain meant that C-59 would further hinder Canada’s national security response.

One such example of legislative overreach extends from discussion about the definitional limits for datasets contrasted against the broad scope of open intelligence available through public and quasi-public sources like social media. Despite C-59’s creation of both the National Security Intelligence Review Agency (NSIRA) and the Intelligence Commissioner (IC), expert witness testimony explored in this thesis continue to elevate the notion that the definition being given for publicly available data does not sufficiently consider Section 8 protections of the

Charter against data holding reasonable expectations of privacy. Considering testimonial accounts from witnesses such as Laura Tribe (OpenMedia) or Lex Gill (Canadian Civil Liberties Association), the broad definitions to what encompasses publicly available data or what datasets can be acquired and retained for exploitation create an environment whereby a conceptual gap exists between what government agencies are afforded to collect against the general public knowledge of how these mandates can affect them. The significance of this can best be explained if we consider the role social media platforms have in relation to publicly available data. As these platforms have continued to evolve and become more ingrained with the social lives of their users, they are more likely to engage in contextual sensitive activities that further increase sharing of information against their own privacy interests (Acquisti, Brandimarte, & Loewenstein, 2015). Despite measures that can be taken to reduce an external online footprint (such as limiting a profile to private), the data that users provide can still be available on the open market such as when Facebook allows their data to be purchased commercially. This research further correlates that notion towards certain excerpts of testimony that calls attention to the supposed elementary knowledge that most Canadians have with regards to what data is public when using IoT and social media despite safeguards that for example require CSIS to eliminate any identifiable information and dispose of datasets past 90 days (unless an extension to retain is authorized).

However, on the other side of this debate was concerns of how motivated threats who are aware of contemporary or developing technology can better leverage these sources to conceal their activities or utilize technology as a compounding factor for cyberattacks. As we saw from testimonial accounts including Lieutenant-General Michael Day or Deputy Chief Laurence Rankin, evolving technology that facilitates device encryption or the increasing use of the cyber-domain in fifth-dimension warfare in their words require that these broader legislative terms be accepted as any restriction or expansion on authorization processes would jeopardize Canada's national security. These testimonies further advanced that the powers being granted in C-59 are more reflective of contemporary society, and that a growing stake in privacy rights is in of itself a required buy-in to participate in it.

If we consider both sides of this issue however, it becomes increasingly apparent how a growing conceptual gap exists when we consider the definitional values being attributed to privacy rights and national security in a digital era. With a rapidly evolving and ever adaptive threat environment becoming increasingly reliant on the fifth-dimension, new and novel methodologies to combatting criminality online will continue to be proposed and implemented on a national scale. However, just as extreme these responses are going to be, so to is a critical examination warranted on the adverse or potentially disproportionate impacts they can have on both innocent populations but also with foreign states, even more so when we consider the international implications something like cyberoperations can have when held against existing agreements such as the Budapest Convention (Couzigou, 2014; Schmitt, 2017). Considering the relatively newness of both IoT and social media, it's drastic expansion and integration into more aspects of everyday lives has provided a boon to companies and governments alike who are able to increasingly gather benign forms of data by its users who may not be able to appreciate just how much inference can be made when parsing them through analytical programs for both commercial and government use.

Discussion: Critical Reflections on Cyber Cold War and the Digital Arms Race

Before discussing final remarks on the more general observations that this study has sought to establish, it's imperative that findings relative to the notions of a rapidly accelerating digitalized arms race be provided dialogue as it can effectively encapsulate microdeviation as an applicable concept towards national security legislation. Throughout the course of this thesis' data collection, it became increasingly apparent that not only was microdeviation viable, but its relationship towards the growing fifth dimension of digitalized warfare and the testimony provided by committee members and expert witnesses provided ample opportunity for comparisons to be made reflective of the Cold War. What that means distinctively is that this study found that testimonial accounts would often weaponize narratives or evidence of the seemingly not so far off or observable capabilities that foreign nation states, particularly China and Russia, have in carrying out attacks on Canada or other allied states for that matter, and that these novel powers akin to cyberoperations and the expansion of digital-based powers including the expansion of big data and dataset exploitation were needed to ensure that Canada is aptly equipped to deal with attacks carried out digitally in the future.

In this context, it's equally important to situate just how pivotal of a role that foreign threats have when leveraging modern technosocial platforms to conduct subtle acts of sabotage that can substantially threaten Canada's national security. As previous scholarly research has demonstrated of foreign cyberthreat capability (Buchanan, 2020; Forrester, Bacovcin, Devereaux, & Bedoya, 2019; Bradshaw & Howard, 2018), this study expanded on theoretical explanations towards examining the utilization of Canadian naivety in the ways that cyberwarfare can be fought via not only discreet sabotage campaigns akin to Stuxnet, but also by weaponizing traditional social media platforms through the use of disinformation campaigns. Given this perspective, this study can provide an example on the rapid pervasiveness that platforms such as social media have when challenging preconceived criminological works examining the connections between individuals and digital technology in conducting deviant or criminal actions. The proliferation of digital platforms including social media and growing concerns of foreign aggressors utilizing them to conduct sabotage campaigns internationally can very well provide an opportunity to rethink the ways that people and technology interact especially given the already prevailing scholarly works that situate how disinformation campaigns through them can provide disproportionate benefits to foreign policy objectives for very little cost.

As my analysis has demonstrated, the threat of foreign states use of these new campaigns to conduct sabotage online and proliferation of advanced IoT technology has effectively heralded a new call for preparatory measures akin to the nuclear arms race that sought a stockpiling of weaponry to be deployed at a moments notice. These calls were observed across multiple individuals who participated in the development of C-59 and notably included Hon. Harjit Sajjan and Hon. Ralph Goodale, two key Liberal MP's that were part of the majority government at the time this bill was tabled. Additionally, this thesis also highlights how certain disproportionate implications such as the impact this modernizing has against Canadian efforts towards maintaining digital privacy online, and how the advancing development of IoT technology further broadens what data can become implicated especially when considering the use of publicly available data in CSIS/CSE intelligence operations. It was also shown that digital privacy, as interpreted through past judicial decisions in Canada, has become more-so a commodity to be leveraged depending on what intelligence agencies require to maintain as testimonial accounts called "cutting-edge" technological capabilities. This is important when we consider the context that this evidence was examined via microdeviations and the disproportionate legislative responses that can occur when considering regulation of online spaces. While this thesis found C-59 as having disproportionate consequences to maintaining anonymity online, testimonial accounts of C-59 continuously framed it as being one that must be acceptable. Against the backdrop of the Cyber Cold War however, this study hopes to have provided a look at how the need to rapidly modify and empower Canada's NSAs based on currently technological trends needs to be based on reasonable temperance and restraint.

Whilst Stuxnet opened the metaphoric pandoras box to weaponizing digital technology and the internet, C-59 could effectively be seen as an extension of this logic via the expanding on developing of new measures towards conducting cybersecurity domestically. That is not to say that the threat capabilities of foreign aggressive states when factoring IoT development and digital sabotage are overestimated, but rather, the integration of Microdeviation Theory into this volatile equation warrants the need to possibly re-think the scale that legislative responses are formed based on contemporary perceptions of technological weaponry and viable near-future developments. Considering testimonial accounts made by most expert witnesses towards the implications of the digital landscape in everyday use as we know it, the exploitation of banal elements of social media platforms and IoT technology by foreign states has thrust Canadian Charter rights as we know it onto centre stage, and whether or not we can effectively develop policy, no less so than national security legislation, against technological prowess with advancements made annually that could effectively nullify any recent bodies of legislation seeking to control them. This is further exacerbated when trying to reconcile growing cyber-threats and the need for Canada to develop and stockpile technological prowess, against section 8 rights as noted previously by Austin (2012) and her commentary towards further trade-offs in digital privacy as contemporary forms of crime surpass written powers that law-enforcement agencies have to respond to it. Considering the advancements that C-59 made towards Canada's NSA review and oversight capabilities with the NSIRA whilst also formally establishing CSE's mandates and providing legislative grounding towards CSIS' intelligence operations, C-59 made clear, positive strides towards embracing a more unified national security strategy. However, this study has also expanded on West's (2018) and Parsons et al. (2017) warnings of the disproportionate implications that weaponizing NSA agencies in cyber-realms can have when factoring in the different ways that cyber-oriented measures can trigger or breach international treaties when compared to traditional, kinetic measures.

Discussion: Final Observations & Future Opportunities

Before concluding this research' discussion, it is vital that the issues pertaining to the inclusion of Brown's (2006) perspective surrounding the criminology of hybrids be afforded examination. Outside of the inclusion of Microdeviation Theory, the underlying theoretical consequences of her analysis towards the unification of person and technology informed most of the criminological implications discussed here. Effectively, Brown's work surrounding technosocial elements to criminal behaviour gives affordance to arguments made here that discuss notions of caution or restraint when basing legislative responses towards digitalized threats. As traditional measures proposed via legislation or control have a continued potential to failure, her work helps to conceptualize the shortcomings that these measures based on dated aspects have when factoring the simple notion that technological advancement, especially in contemporary society, will continue to be out of legislative reach and challenge criminology's traditional role in examining deviancy in binaries. Brown (2006) notes of this dissolving of binaries:

> The increasing ubiquity and complexity of both material and virtual technologies in the production of social order and control in fact suggest this possibility. Transformational interfacing technologies (cybernetics, genetic engineering, digital visualization, satellite

> communications, convergent mobile communications, virtual environments) demand a rethinking of our heavily policed criminological boundaries. We need to dissolve the ‘scientific’ theories and the ‘social’ theories in order to grasp where we are now; and that is immutably in the technosocial. Above all, this is a world where the ‘objects’ and the ‘subjects’, the ‘social’ and ‘scientific’ of criminology’s purview are co-extensive and symmetrically active. (p. 710)

The above excerpt helps to provide a clarification on the line of thinking that this research hopes to address: given this study’s establishment of the narratives used in C-59’s deliberations, the underlying unease of potential developments in the technological sphere, and the established capabilities that foreign or domestic actors have in exploiting technology for the purpose of warfare, it becomes no less so apparent that technological constraints or empowerment based on legislation still tethered to the logic of binaries as Brown (2006) notes might continue to fall short in addressing the reality that the prevalence of IoT technology and platforms such as social media have drastically altered the ways the humans interface with technology to engage in deviant or criminal action. Furthermore, the outstanding evidence contained in this study addressing the proliferation of disinformation campaigns online and their threats to national security serve as additional challenges to scholarly perceptions of cybercrime. Are the actors in these networks leveraging the internet itself as a conduit to disinformation, or is it the leveraging of intimacy and trust that users place in social media platforms in an international actant network? The former here poses questions of the threat actors’ usage of the internet as an extension of themselves to crime, whereas the latter asks of the relationship between the user and the digital landscape as an extension of themselves, yet both revolving around the same concept: the technosocial.

Building off of the concepts mentioned previously, it’s important to also situate the concerns that the criminology of hybrids poses when factoring the 5-year review clause of C-59 that is set to occur in 2024. Touted by Hon. Goodale during the initial hearing on C-59 as being a safeguard against rapidly evolving technology, the clause on face value appears to be conflicting with itself on principle alone when factoring both tenants of microdeviation’s caution against developing legislation based on perceptions of technology rooted in possible fiction, and hybrid criminology’s warning towards binary measures of crime and control. Considering the rapid growth of IoT technology and the pervasiveness in social media platforms online, advancements could feasibly be made before the inevitable review of measures contained in C-59 that will effectively perpetuate the lagging legislative response by Canada’s previous national security legislation except on shorter intervals. Social media and disinformation campaigns alone should serve as a grim example of how foreign aggressors can weaponize the growing integration of the platform’s engagement algorithms with very little barriers to entry but with substantial consequences. The ability to sabotage public discourses on democratic matters and facilitate real-world acts of violence internationally through the simple act of convincing fringe groups through divisive rhetoric far exceeded the perception of foreign state aggression initially during the cold war. If anything, Brown’s (2006) remarks on hybrids can lend credence to the notion that social media and internet platforms have far-exceeded the simple accessory to an individual social life and has instead become a platform that serves as an extension of the physical person into the digital world. However, important to note here is that conclusions cannot be made confidentially at this time given that C-59 was only just enacted and that any further analysis derived from these concepts is far outside the scope of this paper.

CONCLUSIONS

The purpose of this thesis sought to provide a theoretical perspective via the integration of Popham's (2018) Microdeviation Theory that seeks to provide critical context in examining digital capabilities of foreign and domestic aggressors based on the more relatively banal facilities of internet deviancy and subcultures. Beginning at the introduction of C-59 into parliament for consideration, the bills heavy utilization in narratives focusing on the rapidly evolving digital capabilities of threat actors and the new ways that sabotage can be conducted via online channels through either disinformation or weaponizing rapidly evolving IoT technology was seemingly used as the baseline for promoting the modernization and equipping of Canada's NSAs to be "cutting edge" against digitalized threats and the advent of a possible cyber cold war. Specifically, new measures such as the formal establishment of the *Canadian Security Establishment Act*, which brought with it the expansion of their mandate via the addition of the ability to perform active or defensive cyberoperations against cyberthreats, and the solidification of the Canadian Security Intelligence Service's foreign and domestic data collection/retention, saw the majority of concern amongst expert witnesses invited to testify on the structure of the bill (Nesbitt & West, 2019; Nesbitt, 2020; West, 2018). Some of these primary issues consider the role that CSE will now embody as a potential accessory to acts of war via their expansion of the assistance mandate to conducting cyberoperations when granted authority to the Canadian Armed Forces, with West (2018) noting that these new and novel measures being granted to CSE carry with it the potential implication to becoming war-combatants and subject to international treaties governing state self-defence. Additionally, further concerns arise when considering the expanded definition of "publicly available data" as it pertains to state intelligence operations especially against the backdrop of a growing IoT economy that increasingly encroaches

Canadian user data to function, subjecting previously intimate data to the possibility of being sold on the public market.

Additionally, the findings of this thesis also have importance towards how the outwardly portrayal of one's social life online and ignorance of privacy will continue to affect cultural opinions towards the balancing of Charter rights against increasingly aggressive national security measures. Findings from this thesis help support and build on existing scholarly research surrounding the advent of disinformation campaigns online by providing Microdeviation Theory as a new perspective to examining relatively banal behaviours online such as the social "hacking" on social media platforms to advance foreign disinformation and affect Canada's social cohesion. The propositions of Microdeviation Theory advance that foreign adversaries will leverage IoT technology and social media online to perpetuate disinformation across borders in the hopes of undermining Canadian's belief in democratic institutions and naivety towards the threats that can occur online and translate into offline violence. This research helped to provide further exploration and application of the concept by examining the expert witness responses to C-59's expansion of CSIS and CSE's mandates including the formalization of bulk data collection or providing CSE with the legislative authority to become a more pro-active agency in the fight against threats online. The most prominent example of potential responses came in the form of expanding CSE's mandate to include both active and defensive cyberoperations, a new and untested design of conducting cybersecurity that saw expert witness testimony align with previous scholarly work on C-59 that warns of potential implications towards legislating state-sponsored surveillance and the chilling effects towards international relations (Nesbitt & West, 2019; West, 2018; Parsons, Gill, Israel, Robinson, & Deibert, 2017). Furthermore, this research expands on West's (2018) works examining the potential implications towards international treaties by situating Microdeviation Theory as a unique perspective that can provide a baseline approach to rethinking cyber-focused legislation and challenging current preconceptions of the relationship between physical bodies and the technosocial as cyber-focused national security strategies become more commonplace and present far-reaching consequences via the implication of CSE in acts of war. However, given that C-59 effectively modernized both CSIS and CSE's mandates that was previously rooted in decades old legislation, a more proper examination of how publicly available data or data willingly posted or sold online should be defined could be explored in the future given that a study of that undertaking is well beyond the scope of this research.

This thesis additionally provides critical qualitative documentation highlighting how a proliferation of new and novel ways to conducting terrorism online with the utilization of IoT technology and the Internet with the justification of developing more aggressive measures digitally to preserve Canada's borders and is partially indicative of previous work conducted by Arayankalam and Krishnan's (2021) research establishing how governments may utilize the threat of social media disinformation campaigns to acquire further control of domestic media groups to contain its spread. Furthermore, it is noted here that these findings further align with Wall's (2008) remarks surrounding the controlling stake that science-fiction portrayals of technology can have with swaying public opinion on matters concerning the fight against cyber-threats.

While qualitative evidence was found across testimony to support notions of the concept, the obvious lack of further elaboration on specifics pertaining to what types of technology supposedly being developed mean that this study's full connection between the 2 concepts (manufactured uncertainty and terrorist/foreign state technological capabilities) is effectively constrained, but reasonable given how national security strategies require secrecy and discreteness to be effective. These limitations contrast to the findings of Bradshaw and Howard (2018) who noted that the lack of data surrounding misinformation campaigns and the modal-actors who perpetuate them effectively makes "painting a complete picture of these activities by government actors" an extremely difficult task with these gaps in data (p.29). However, the integration of Microdeviation Theory here has provided an additional perspective to examining the complexities of manufactured uncertainty towards a multitude of aspects reflective of social media technology and the growing use and development of IoT products and what narratives democratic governments may use when discussing the possible adverse effects towards a nation's sovereignty.

Given this context, the integration of both Microdeviation and technosocial concepts towards evidence given by expert witness testimony helps to expand on scholarly work before it considering cybercrime, but also attributes itself as an integration into the growing publications surrounding the effects that disinformation campaigns via social media carry against traditionalist ways of conducting aggression or sabotage against the international community at large (Arayankalam & Krishnan, 2021). Focusing on testimony considering digital advancement and the growing IoT economy online, the application of Microdeviation Theory highlights the notion that Canadian adaptation of the digitalized economy and social media is still one that is faced with naivety and is therefore subject to subversion via unconventional exploitation and normalized elements pertaining to the true extent of maintaining privacy online or being equipped to properly combat disinformation online.

APPENDIX

MEETING DATE	WITNESSES	INDUSTRY
November 30, 2017	Ralph Goodale Greta Bossenmaier Dominic Rochon David Vigneault Vincent Rigby Kevin Brosseau Douglas Breithaupt	Minister of Public Safety Chief, CSE Deputy Chief of Policy and Communications, CSE Director, CSIS Deputy Minister (Public Safety) Deputy Commissioner (RCMP) Department of Justice
December 5, 2017	Alex Neve Craig Forcese Stephanie Carvin Wesley Wark	Secretary General, Amnesty International Canada Individual, Carleton University Individual, University of Ottawa Individual, University of Ottawa
December 7, 2017	Brenda McPhail Cara Zwibel Lex Gill Daniel Therrien Patricia Kosseim Lara Ives Christian Leuprecht Hayley McNorton	Director, Canadian Civil Liberties Association Acting General Counsel, Canadian Civil Liberties Association Advocate, Canadian Civil Liberties Association Privacy Commissioner of Canada Senior General Counsel, Office of the Privacy Commissioner Acting Director General, Office of the Privacy Commissioner Individual, Royal Military College of Canada Research Assistant, Royal Military College of Canada
December 12, 2017	Ishaan Gardee Faisal Bhabha Zamir Khan Khalid Elgazzar Shimon Fogel Kent Roach	Executive Director, National Council of Canadian Muslims Legal Advisor, National Council of Canadian Muslims Parent, No Fly List Kids Lawyer, No Fly List Kids CEO, Centre for Israel and Jewish Affairs Individual, University of Toronto
January 30, 2018	Jean-Pierre Plouffe J. William Galbraith Gerard Normand Micheal Vonn Raymond Boisvert	Commissioner, CSE Commissioner Executive Director, CSE Commissioner Legal Advisor, CSE Commissioner Policy Director, British Columbia Civil Liberties Association Deputy Minister, Ontario Ministry of Community Safety
February 1, 2018	Peter Edelmann Gillian Carter Paul Martin Laurence Rankin Christina Szurlej	Member at Large, Canadian Bar Association Staff Lawyer, Canadian Bar Association Chief, Durham Regional Police Services Deputy Chief Constable, Vancouver Police Department Individual, St. Thomas University
February 6, 2018	Denis Barrette Dominique Peschard Pierre Blais Chantelle Bowers Richard B. Fadden Faisal Mirza	Spokesperson, Lique des droits et libertés Spokesperson, Lique des droits et libertés Chair, Special Intelligence Review Committee Acting Executive Director, Special Intelligence Review Committee Individual Chair, Canadian Muslim Lawyers Association
February 8, 2018	Michael Mostyn David Matas Timothy McSorley Laura Tribe Michael Nesbitt	CEO, B'nai Brith Canada Senior Legal Counsel, B'nai Brith Canada National Coordinator, International Civil Liberties Monitoring Group Executive Director, OpenMedia Individual, University of Calgary

February 13, 2018	Malcolm Brown	Deputy Minister, Department of Public Safety
	John Davies	Director General, Department of Public Safety
	Shelly Bruce	Associate Chief, CSE
	Scott Millar	Director General, CSE
	Tricia Geddes	Assistant Director, CSIS
	Merydee Duthie	Special Advisor, CSIS
	James Malizia	Assistant Commissioner, RCMP
	Gilles Michaud	Deputy Commissioner, RCMP
	Douglas Breithaupt	Director and General Counsel, Department of Justice
February 15, 2018	Guy Bujold	Interim Vice-Chairperson, Civilian Review and Complaints Commission
	Joanne Gibb	Director, Civilian Review and Complaints Commission
	Michael Day	Individual, Lieutenant-General (Retired)
	Scott Newark	Individual, Policy Analyst
March 22, 2018	Harjit Sajjan	Minister of National Defence
	Richard Feltham	Director General, Department of National Defence
	Stephen Burt	Assistant Chief of Defence Intelligence, Department of National Defence
	Greta Bossenmaier	Chief, CSE
	Shelly Bruce	Associate Chief, CSE
	Scott Jones	Deputy Chief, CSE
	Dominic Rochon	Deputy Chief, CSE
April 17, 2018	Douglas Breithaupt	Director and General Counsel, Department of Justice
	John Davies	Director General, Department of Public Safety
	Sophie Beecher	Director of Intelligence Policy, Department of Public Safety
	Cherie Henderson	Director General, CSIS
	Scott Millar	Director General, CSE
April 23, 2018	Douglas Breithaupt	Director and General Counsel, Department of Justice
	John Davies	Director General, Department of Public Safety
	Sophie Beecher	Director of Intelligence Policy, Department of Public Safety
	Cherie Henderson	Director General, CSIS
	Scott Millar	Director General, CSE
	Charles Arnott	Manager of Strategic Policy, CSE

BIBLIOGRAPHY

42nd Parliament. (2017). *Standing Committee on Public Safety and National Security*. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-90/minutes

42nd Parliament. (2017). *Standing Committee on Public Safety and National Security*. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-89/minutes

42nd Parliament. (2017). *Standing Committee on Public Safety and National Security*. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-88/minutes

42nd Parliament. (2018). *Standing Committee on Public Safety and National Security*. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-98/minutes

42nd Parliament. (2018). *Standing Committee on Public Safety and National Security*. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-101/minutes

42nd Parliament. (2018). *Standing Committee on Public Safety and National Security*. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-93/minutes

42nd Parliament. (2018). *Standing Committee on Public Safety and National Security*. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-94/minutes

42nd Parliament. (2018). *Standing Committee on Public Safety and National Security*. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-101/minutes

42nd Parliament. (2018). *Standing Committee on Public Safety and National Security*. Retrieved from https://www.ourcommons.ca/DocumentViewer/en/42-1/SECU/meeting-96/minutes

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and Human Behavior in the Age of Information. *Science*, 509-514.

Andrejevic, M., & Gates, K. (2014). Big Data Surveillance: Introduction. *Surveillance & Society*, 185-196.

Arayankalam, J., & Krishnan, S. (2021). Relating foreign disinformation through social media, domestic online media fractionalization, government’s control over cyberspace, and social media-induced offline violence: Insights from the agenda-building theoretical perspective. *Technological Forecasting & Social Change*, 1-14.

Austin, L. M. (2007). Information Sharing and the 'Reasonable' Ambiguities of Section 8 of the Charter. *The University of Toronto Law Journal*, 499-523.

Austin, L. M. (2012). Getting Past Privacy? Surveillance, the Charter, and the Rule of Law. *Canadian Journal of Law and Society*, 381-398.

Austin, L. M. (2015). Lawful Illegality: What Snowden Has Taught Us About the Legal Infrastructure of the Surveillance State. In M. Geist, *Law, Privacy, and Surveillance in Canada in the Post-Snowden Era* (pp. 103-125). Ottawa: University of Ottawa Press.

Bailey, J. (2012). Systematic government access to private-sector data in Canada. *International Data Privacy Law*, 207-219.

Bradshaw, S., & Howard, P. N. (2018). The Global Organization of Social Media Disinformation Campaigns. *Journal of International Affairs Editorial Board*, 23-32.

Brown, S. (2006). The Criminology of Hybrids: Rethinking Crime and Law in Technosocial Networks. *Theoretical Criminology*, 223-244. Retrieved from https://journals.sagepub.com/doi/10.1177/1362480606063140

Buchanan, T. (2020). Why do people spread false information online? The effects of message and viewer characteristics on self-reported likelihood of sharing social media disinforamtion. *PLoS ONE*, 1-33.

Cain, P. (2019, January 30). Feds Unveil Plan to Fight Foreign Interference in 2019 Federal Election. *Global News*. Retrieved from https://globalnews.ca/news/4905368/foreign-election-interference-canada/

Conrod, L.-A. (2019). Smart Devices in Criminal Investigations: How Section 8 of the Canadian Charter of Rights and Freedoms can Better Protect Privacy in the Search of Technology and Seizure of Information. *Appeal*, 115-133.

Couzigou, I. (2014). The Challenges Posed by Cyber Attacks to the Law on Self-Defence. *European Society of International Law, 16*, pp. 1-16. Vienna.

Critical Appraisal Skills Programme. (2018). *CASP Qualitative Checklist.* Retrieved from https://casp-uk.b-cdn.net/wp-content/uploads/2018/03/CASP-Qualitative-Checklist-2018_fillable_form.pdf

CSE. (2018). *National Cyber Threat Assessment 2018.* Ottawa: Government of Canada. Retrieved from https://www.cyber.gc.ca/en/publications

CSE. (2019). *2019 Update: Cyber Threats to Canada's Democratic Processes.* Ottawa: Government of Canada.

CSIS. (2018). *Who Said What? The Security Challenges of Modern Disinformation.* Ottawa: Government of Canada.

Daniels, J. (2018). The Algorithmic Rise of the Alt-Right. *Contexts*, 60-65.

Forrester, B., Bacovcin, A., Devereaux, Z., & Bedoya, S. (2019). *Propaganda Filters: Tracking Malign Foreign Interventions on Social Media.* S&T Organization. Retrieved from http://www.datametrex.com/investor/nato-report.html

Gable, K. A. (2010). Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent. *Vanderbilt Law Review*, 57-118.

Graebner, N. A. (2000). Myth and Reality: America's Rhetorical Cold War. In M. J. Medhurst, & H. W. Brands, *Critical Reflections on the Cold War: Linking Rhetoric and History.* Texas: Texas A&M University Press.

Hunter v. Southam, 17569 (S.C.C. November 22, 1984).

Kierkegaard, S. M. (2005). Cracking Down On Cybercrime Global Response: The Cybercrime Convention. *Communications of the IIMA*, 59-66.

Laurin, P. (2020). Gerrymandering the National Security Narrative: A Case Study of the Canadian Security Intelligence Services' Handling of its Bulk Metadata Exploitation Program. *Surveillance & Society,* 370-386.

Lee, H. (2005). Behavioral Strategies for Dealing With Flaming in an Online Forum. *The Sociological Quarterly, 46,* 385-403.

Lewis, R. (2018). *Alternative Influence: Broadcasting the Reactionary Right on Youtube.* Data & Society. Retrieved from https://datasociety.net/library/alternative-influence/

Lyon, D. (2015). *Surveillance After Snowden.* Cambridge: Polity Press.

Maras, M.-H. (2015). Internet of Things: Security and Privacy Implications. *International Data Privacy Law*, 99-105.

Maras, M.-H. (2017). Overcoming the intelligence-sharing paradox: Improving information sharing through change in organizational culture. *Comparative Strategy*, 187-197.

Marwick, A., & Lewis, R. (2017, May 15). Media Manipulation and Disinformation Online. pp. 1-104.

Massanari, A. (2017). #Gamergate and The Fappening: How Reddit’s algorithm, governance, and culture support toxic technocultures. *New Media & Society, 19*(3), 329-346.

McCombie, S., Uhlmann, A. J., & Morrison, S. (2019). The US 2016 presidential election & Russia’s troll farm. *Intelligence and National Security*, pp. 1-20.

Nagle, A. (2017). *Kill All Normies: Online Culture Wars from 4chan and Tumblr to Trump and the Alt-Right.* Alresford: John Hunt Publishing.

Nesbitt, M. (2020). Reviewing Bill C-59, An Act Respecting National Security Matters 2017: What's New, What's Out, and What's Different From Bill C-51, A National Security Act 2015? *Canadian Global Affairs Institute,* 1-37.

Nesbitt, M., & West, L. (2019). Bill C-59, An Act Respecting National Security Matters: What It Does and Why It Matters. *Alberta Law Review*, 165-174.

Parsons, C., Gill, L., Israel, T., Robinson, B., & Deibert, R. (2017, December). Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading (December 18, 2017).

Patry, W. (2009). *Moral Panics and the Copyright Wars.* Oxford University Press.

Popham, J. (2018). Microdeviation: Observations on the Significance of Lesser Harms in Shaping the Nature of Cyberspace. *Deviant Behaviour, 39*(2), 159-169.

Porteous, H. (2018). *Cybersecurity: Technical and Policy Challenges.* Ottawa: Library of Parliament.

R v. Plant, 22606 (S.C.C. November 5, 1992).

R v. Tessling, 29670 (S.C.C. April 16, 2004).

Riga, A. (2018, Apri; 23). Inside The Life of Quebec Mosque Killer Alexandre Bissonnette. *Montreal Gazette*. Retrieved from https://montrealgazette.com/news/local-news/alexandre-bissonnette-inside-the-life-of-a-mass-murderer

Roach, K., & Forcese, C. (2015). *False Security: The Radicalization of Canadian Anti-Terrorism.* Toronto, Ontario: Irwin Law Inc.

Saldaña, J. (2014). Coding And Analysis Strategies. In P. Leavy, *The Oxford Handbook of Qualitative Research* (p. 756). New York: Oxford University Press.

Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* New York: Cambridge University Press.

Scrivens, R., Davies, G., & Frank, R. (2018). Measuring the Evolution of Radical Right-Wing Posting Behaviors Online. *Deviant Behavior*, 1-17.

Stahl, W. M. (2012). THE UNCHARTED WATERS OF CYBERSPACE: APPLYING THE PRINCIPLES OF INTERNATIONAL MARITIME LAW TO THE PROBLEM OF CYBERSECURITY. *GA. J. INT'L & COMP. L.*, 247-273.

Take, I. (2012). Regulating the Internet Infrastructure: A Comparative Appraisal of the Legitimacy of ICANN, ITU, and the WSIS. *Regulation & Governance, 6*, 499-523.

Taylor, J. (2016). Minding the Gap: Why or How Nova Scotia Should Enact a New Cyber-Safety Act - Case Comment on Crouch v. Snell. *Canadian Journal of Law and Technology, 14*(1).

Tunney, C. (2019, April 10). CSIS dealing with right-wing extremism 'more and more,' says spy chief. *CBC News*. Retrieved from https://www.cbc.ca/news/politics/csis-right-wing-white-supremacy-1.5092304

Van Dine, A. (2020). When is Cyber Defense a Crime? Evaluating Active Cyber Defense Measures under the Budapest Convention. *Chicago Journal of International Law*, 530-564.

West, L. (2018). Cyber Force: The International Legal Implications of the Commuication Security Establishment's Mandate under Bill C-59. *Canadian Journal of Law and Technology, 16*, 381-416.

West, L., & Forcese, C. (2019). Building Haystacks: Information Retention and Data Exploitation by the Canadian Security Intelligence Service. *Alberta Law Review*, 175-202.