uOttawa

ÉSAPI GSPIA École supérieure d'affaires publiques et internationales
Graduate School of Public and International Affairs

MAJOR RESEARCH PAPER

GOVERNMENT-MEDIA RELATIONS IN CANADA'S FEDERAL CYBER SECURITY (JULY - DECEMBER 2018 & 2021)

Victoria Lopez
Email Address: vlope087@uottawa.ca
Student Number: 4606082
Date: August 12, 2022

Contents

List of Figures

Abstract

The world is increasingly technologically connected, and those technologies are advancing at rapid pace, meaning that cyber security can seem like whack-a-mole. Malicious cyber activity plays heavily in geopolitics and governments worldwide are faced with challenges to protect their citizens and sovereignty. This research evaluates the Government of Canada's approach to communicating with the public about cyber security activities and programming based on representations in traditional news media. It develops a model of government-media relations in federal cyber security activities and programming based on cross-sectional analysis of two six-month periods (from July – December in 2018 and 2021). These periods correspond to the six months following the release of Canada's most recent highest-level strategy for cyber security, the National Cyber Security Strategy, and a contemporary period. It assesses the representations and analyzes some relevant themes throughout like the Huawei 5G story that spans the timeframe. This is largely an assessment of what gets picked up in traditional news media and contextually why that is. There appeared to be a predominantly information dissemination model of government-media relations which neither favoured or dissented the Government of Canada's activities and programming in cyber security. There was some evidence of a two-way asymmetric model, but this could not be determined within the scope of this analysis in evaluating traditional news media content.

List of Acronyms

AI – Artificial Intelligence

CCCS – Canadian Centre for Cyber Security

CRTC – Canadian Radio-television and Telecommunications

CSE – Communications Security Establishment

CSIS – Canadian Security Intelligence Service

GC – Government of Canada

IoT – Internet of Things

NATO – North Atlantic Treaty Organization

NCSS – National Cyber Security Strategy

NSAP – National Cyber Security Action Plan

RCMP – Royal Canadian Mounted Police

USMCA – United States-Mexico-Canada Free Trade Agreement

Introduction

A primary concern for the Government of Canada (GC) is securing Canadians but doing so has become increasingly complex as the threat landscapes continue to evolve. While cyber security was already a prominent issue, it has become even more so with COVID-19 forcing more activity online highlighting the urgency. Cyber security encompasses traditional technologies (telephony, information management/information technology systems, and networks), cloud-based technologies, as well as emerging technologies like artificial intelligence (AI), the Internet of Things (IoT), blockchain, and quantum computing. It also entails human factors across public and private sectors as well as Canadians themselves as end users.

In a complex and evolving cyber threat environment, how do governments communicate cyber security activities and programming to the public? This study looks at the case of Canada through traditional news media analysis using cross-sectional data across two periods to develop a model of government-media relations for GC cyber security. The two periods are from July – December in 2018 and 2021 to include six months after the 2018 National Cyber Security Strategy (NCSS) was released and a corresponding contemporary period in 2021. These periods were selected as the NCSS is the highest-level cyber security strategy for the GC to evaluate the corresponding work in news media representations. What became evident was that most of the GC's activities in cyber security were not covered by news media and in each period a select few key themes were dominant with a sprinkling of other topics throughout. Often with cyber security when things are going well, they are happening behind the scenes so it's like many medical tests where no news is good news. A lot of the complex technical programs

and activities that the GC undertook in cyber security were not communicated. Instead, there were several high publicity stories that caught the attention of multiple sources over the timelines. The Huawei 5G storyline was prevalent in both periods as were themes of foreign interference via elections meddling, disinformation, cyberattacks, espionage, and intellectual property theft. These were largely attributed to China and Russia. Other key themes were ransomware, cyber crime, and critical infrastructure attacks. Most articles included GC speaking points in both periods, which was indicative of a symbiotic relationship between the GC and news media. The GC is reliant on news media to get messaging out, but journalists are also reliant on the GC for a steady stream of reliable information (Pearson & Patching, 2008) on cyber security activities. The representations were predominantly neutral, which indicates that the news media was neither dominated by promotions nor critiques of the GC. When there was a sway, it was more often negative on the GC.

How GC cyber security activities and programming are communicated with the public can impact their uptake, effectiveness, and engender or dissuade the public trust. This is incredibly important to preserving democratic order because cyber security is a team sport. Any device that connects to the internet, is plugged into a public USB port, or has tappable purchasing is a potential penetration point or vulnerability. Having the public engaged increases Canada's overall cyber resilience. General awareness of cyber hygiene, best practices, and GC programming or points of contact to report malicious activity can reduce public risk and support the GC in addressing cyber incidents. Moreover, some cyber attacks target the public psyche. Successful disinformation campaigns can dissuade the public trust in the GC and increase political polarization. The

representation of GC cyber security programs and activities as demonstrated in traditional news media sources is an indicator of the effectiveness of GC communications. Through developing a model of government-media relations and evaluating representations of the GC's activities and programming in cyber security it is possible to develop recommendations for improved public engagement in the GC's cyber security ambitions.

The GC only controls a finite portion of the communications that the public receives on cyber security. People get their information from many sources, including social media, and face digital misinformation campaigns in the process. The relationship between AI, governance, human rights, and digital security is a key theme in cyber security. Aside from AI technologies that are anthropomorphized leading to biased results, AI is also being leveraged by those with divergent views to Canada for digital misinformation campaigns (Wilner, 2018). This creates a complicated information space that is difficult for the public to navigate. Cyber security can be highly technical and complicated to understand for a general audience already without having confounding narratives from disinformation campaigns.

While the GC provides information directly to the public across an array of settings, including public-facing websites, reports, White Papers, press statements, social media releases, and via conferences or forums the GC messaging can get lost in the masses of information. Therefore, how the news media portrays the GC's efforts on cyber security can serve to encourage or deter public trust. A free press is a fundamental democratic institution protected in Canada under Section 2(b) of the Canadian Charter of Rights and Freedoms (Government of Canada, 2021). "[A] democratic political system cannot function without diverse, free, and independent sources of news" … "one of the functions

of news and journalism is to keep up the accountability of governments, business and individuals" (Organisation for Economic Co-operation and Development, 2010).

The GC's relationships with news media can influence the extent to which and how GC messages, strategies, policies, and programs get represented. As a major source of information for the public on the GC's activities in cyber security, the prevalent model of government-media relations can sway public opinion, which in turn can in turn impact upon the GC's capacity to effectively serve the public. The model of government-media relations evaluated herein is based strictly on traditional news media sources. These are held to a level of accountability unlike the limited capacity to control social media sources. In Canada there are self-regulating ethics bodies for the news media industry, including the National NewsMedia Council (National NewsMedia Council, 2021) and the Quebec Press Council (Quebec Press Council, n.d.) as well as the Canadian Association of Journalists (Canadian Association of Journalists, 2011) holding journalists accountable to ethics standards.

The research and analysis are presented across several sections starting with a Background Literature Review detailing some of the relevant GC programming and accountabilities in cyber security with context for government-media relations models. With that background, the Research Purpose and Model are presented followed by a Design and Methodology section for identifying the specific government-media relations model for the GC on cyber security. Results Analysis is then provided for the 2018 and 2021 periods followed by cross-sectional analysis. The work closes with Conclusions and Recommendations, including possible future research areas.

Background Literature Review

Regardless of GC policy or program there will be supporters and dissenters. The extent to and context within which the GC is represented in news media is an indicator of the model of government-media relations. This provides a pulse on the interface between journalism and the executive – both of which are fundamental democratic institutions (Pearson & Patching, 2008). The GC's cyber security policies and programs are a Team Canada project spread across a multiplicity of actors in an array of domains. Below is a high-level overview of some key GC's actors, activities, and accountabilities followed by a brief background on government-media relations models to frame analysis.

Brief Overview of GC Cyber Security Actors, Activities, and Accountabilities

Public Safety Canada oversees the NCSS 2018, which funded and provided accountabilities to several other departments to address cyber concerns in the NCSS. The plan included working with provincial and territorial governments and the private sector (Public Safety Canada, 2018). The three themes for the GC and its partners include security and resilience, cyber innovation, as well as leadership and collaboration. This was to build on the work achieved by the original NCSS from 2010 that focused on security of GC systems, partnering to secure vital cyber systems outside of the federal government, and helping Canadians to be secure online. It took stock of a changing landscape with evolving threats in cyberspace. Goals set forth were secure and resilient Canadian systems, effective leadership and collaboration, along with an innovative and adaptive cyber ecosystem (Public Safety Canada, 2018). As the lead on NCSS 2018 Public Safety Canada oversees the implementation, including the National Cyber Security Action Plan (NSAP) 2019-2024 (Public Safety Canada, 2019).

Communications Security Establishment (CSE) is the technical authority for cyber security, the lead on cyber operations and foreign signals intelligence, and houses the Canadian Centre for Cyber Security (CCCS) (Public Safety Canada, 2020). CCCS performs cyber security validation for telecommunications and associated technologies (Canadian Centre for Cyber Security (CCCS), 2018). This is particularly relevant to a key theme throughout on Canada's decision-making on Huawei in 5G (Zimonjic, 2021). CCCS has led in Canada's public attributions of foreign state actor involvement in malicious cyber activity across the time periods. They perform intelligence analysis and provide public reporting on the status of cyber security-related activities and statistics such as information about ransomware (Canadian Centre for Cyber Security (CCCS), 2020). CCCS provides guidance to the GC, businesses, and the Canadian public on keeping cyber secure and mitigating cyber threats (Canadian Centre for Cyber Security (CCCS), 2021), including "[b]aseline cyber security controls for small and medium organizations" (Canadian Centre for Cyber Security (CCCS), 2021) and the Get Cyber Safe national public awareness campaign to inform Canadians about cyber security and how to protect themselves online (Canada, 2022). Given the role of public communications for CSE and CCCS in these tasks how effectively they are presented in news media is important.

Public Safety Canada's NSAP 2019-2024 set specific goals and tasks departments and agencies with roles in federal cyber security management. Actions and milestones are outlined for Public Safety Canada, CSE, Canadian Security Intelligence Service (CSIS), Royal Canadian Mounted Police (RCMP), Employment and Social Development Canada, Natural Resources Canada, Global Affairs Canada, and Innovation, Science, and Economic Development Canada (Public Safety Canada, 2019). Many other

organizations also have roles to play in cyber security in Canada, including Department of National Defence, Defence Research and Development Canada, Treasury Board of Canada Secretariat, Shared Services Canada, Canadian Radio-television and Telecommunications Commission (CRTC), the Office of the Privacy Commissioner of Canada, and the Canadian Anti-Fraud Centre (Public Safety Canada, 2020). With all these players involved analysis included whether specific department or agency activities or messages were mentioned and how they/their work was being represented.

Background on Government-Media Relations Models

What can be learned through applying a lens of government-media relations models to analysing communications on the GC's cyber security programming and activities? Some elements include an indication of the freedom of the press as well as effectiveness of GC communications in reaching a broad public audience. The analysis can identify whether the GC has capture over traditional news media as some pundits would decree, if instead traditional news media provided a challenge function with critical counter-GC messaging, or if the approach was more of a neutral fact presentation.

Political communications and government-media relations have been studied by researchers across a range of disciplines including politics, history, sociology, media studies, cultural studies, and communication (Pearson & Patching, 2008). Some models for government-media relations are drawn from public relations theory. Interestingly the predominant public relations models are the same four from Grunig and Hunt's developed in 1984 but with theory built out over time. One-way communication models include publicity (press agentry) and dissemination of information (public information). Publicity relies upon generating media hype with minimal consideration for veracity. Dissemination

of information comes from a writer representing clients and issuing news releases (Saylor Foundation, 2016). Under these models, the stories are driven by the source. The two-way communication models are asymmetrical and symmetrical. Asymmetrical has evolved to include principles of behavioural psychology as the public relations seeks to understand what publics know, understand, or believe about the client (GC in this case), which is then incorporated into the messaging. The communicator has greater power for intelligence to inform communications in an asymmetrical model. The symmetrical model also leverages public opinion research, but instead of persuasion seeks to develop a mutual understanding between the publics and client (Saylor Foundation, 2016).

It was important to evaluate the extent to which the press was free or if there was an apparent level of GC capture. Robin Brown defined political spin as “form of interaction between press officers and journalists governed by a set of mutually accepted rules and a proactive approach to political relations that seeks to maximise favourable coverage” (Pearson & Patching, 2008). Periodicals and series of articles will be assessed for political spin. Further evidence of this activity can be found in evaluating another theory. Eric Louw developed the “Spiral of Silence” theory based upon a “sensible centre” composing the majority of stories and those with ideas or people threatening to the “sensible centre” end up not reported or reported with a sneer to indicate to audiences that the “ideas were extreme and unacceptable” (Pearson & Patching, 2008).

Research Purpose, Design, and Methodology

Purpose

The purpose of this research was to evaluate the representation of Canadian federal policy, programming, activities, and initiatives in cyber security within traditional

Canadian news media. It focused strictly on traditional news media sources for the sake of breadth of reach, the editorial process requiring content be vetted, and existing relationships with the GC. The intent was to develop a well-rounded model of government-media relations as it pertained to GC cyber security activities, policies, programs, and initiatives across two periods. This provided insights within each period, between the two, and generally how the GC fared in the public eye across a range of GC cyber security activities.

Design

Modelling GC government-media relations in cyber security supported analysis on freedom of the press (a fundamental tenant of democracy), the extent to which the GC leverages news media to communicate with the public, high visibility topics for GC cyber security, and public perceptions of the GC's activities in this area. It also provided indications for whether the GC had the public trust in cyber security based on whether representations were positive, negative, or ambiguous across given storylines.

The GC's cyber security representation in traditional news media sources was evaluated against different forms of government-media relations models. These included one-way, two-way, symmetrical, and asymmetrical communications approaches detailed above in the Background Literature Review. There were also contextual factors to the time periods that impact the modelling. Journalists may depend on "government sources for a steady, reliable, cost-effective and credible flow of news" creating a symbiotic relationship (Pearson & Patching, 2008). Increasingly, traditional news media must compete with social media or free content sources for viewership which can limit funding. This could mean less resources with journalists spread thinly on a broad range of issues.

Methodology

This research is a government-media relations cross-sectional case analysis on GC cyber security programs and activities, and it refers to contextual factors. It evaluates two six-month periods to represent the period immediately after the June 2018 announcement of the new NCSS as the highest-level strategy for the GC (Government of Canada, 2018) and a contemporary period (July – December 2018 & 2021). Since the announcement and implementation, the GC has had a lot of activity related to cyber security. Some of this was detailed in the Background Literature Review and more is elaborated upon below. How this was represented in news media in each period and across both periods is assessed herein.

Extensive content review from GC sources and traditional news media sources supported the research. Review of policy documents, websites, public statements, press releases, and other publicly available documentation helped to identify GC activity on cyber security. A sample of newspaper articles from the two periods addressing GC cyber security activities was evaluated from the following news media sources: the *Ottawa Citizen, The Globe and Mail*, the *National Post*, the *Toronto Star*, *La Presse*, and *Le Droit*. These were gathered through a database review in Factiva and Eureka to collect articles based on keyword searches across headlines, abstracts, and full text of articles using search terms identified in Appendix A – Search Terms.

Articles that did not pertain specifically to GC cyber security were filtered out and the rest were evaluated against a range of qualitative criteria to support this analysis. For example, a major thread across periods involved Huawei's 5G technology, Chinese cyber hacking, the arrest of Ms. Meng, the subsequent detention of two Canadians in China,

and the ultimate release of all three parties (Zimonjic, 2021). This story had many dimensions and is scoped herein to exclude articles that strictly pertained to foreign relations or negotiations for detainees without GC cyber security-specific content. Likewise, articles about the WeChat red dot hiding articles with negative opinions on Huawei to Canadians (Nutall & Chiu, 2018) were not included if there was no reference to GC cyber security programs or activities.

The complete question codification is provided in Appendix B – Qualitative Content Analysis Framework. However, some of the main elements evaluated are detailed below.

1. Within which context is the representation of the GC's actions in cyber presented (positive, negative, neutral, or ambiguous)? This was assessed through headlines, abstracts, and body text of news articles.
2. Whose perspectives are being represented and whether they are generally aligned to or critical of the GC, which specific policies, programs, activities, and initiatives are highlighted, and whether speaking points or other GC content are included.
3. A binary variable was included on whether links were provided to GC sources.
4. Articles were categorized and analyzed based on the type of cyber security concern addressed (e.g., strategic direction, programs, policies, procurement, international cooperation, public attributions of malicious cyber activity, emerging technology, etc.) to assist in identifying key themes and to determine what received the most attention.
5. The research evaluated departments, agencies, or political figures represented and whether they were presented in a positive, negative, neutral, or ambiguous manner.
6. Responses for questions assessing positive, negative, or ambiguous skew were reviewed for absolutist language leveraged to qualitatively frame the articles. Where

applicable, additional context was identified for these nuances. Articles were analyzed to determine whether there are indications of spin as proactive political relations to maximize favourable coverage or a spiral of silence (Pearson & Patching, 2008).

Through this analysis a model of government-media relations was developed for the GC, but there are certain weaknesses to this methodology. It is difficult to draw inferences on the two-way communications models (asymmetrical or symmetrical) without access to internal GC documentation like surveys, polling, outreach and engagement strategies, or communications plans. Not including social media, podcasts, or other sorts of media might miss some demographics that do not follow traditional news media sources, but that would vastly expand the scope. There are also limitations to a cross-sectional analysis using these two periods. The original NCSS was released in 2010 (Public Safety Canada, 2018) so this analysis will not capture the media representations of the initial phase of work in this domain. The research might miss major events in the gap between periods or after the last period. For example, as the contemporary period needed to be time bounded the GC's response to the exploitation of Apache Log4j vulnerability (Canadian Centre for Cyber Security (CCCS), 2021) only included the beginning of GC cyber security response. It also completely misses the GC response to the Follina vulnerability impacting Microsoft products (Canadian Centre for Cyber Security (CCCS), 2022). The recent Rogers outage that left Canada Border Services Agency's ArriveCAN application and Service Canada's offices and call centres (including passport offices), Interac services, major financial institutions, and multiple police services impacted (Da Silva & Augustin, 2022) was also outside of scope. Cyber

security keeps evolving though and with the parameters of a Major Research Paper limitations needed to be set but there are some important insights.

Results and Analysis

2018 Summary

2018 news media sources had 192 articles analyzed from July – December. 94 of these were from *The Globe and Mail* at almost three times any other news media source (per Figure 1 below). Several factors that may have contributed to this include that *The Globe and Mail* reposts articles from the *National Post* or *Financial Post* (under the same umbrella) frequently with slightly different versions which varying in size, focus, speaking points included, and/or title as well as the practice of summary wrap-up evening updates.

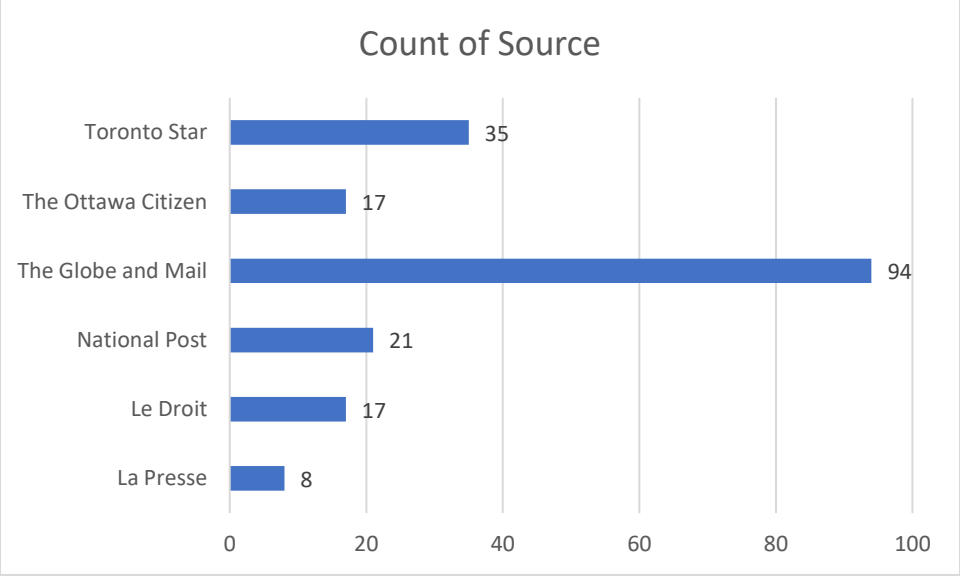

Figure 1: 2018 Count of Source References

Following *The Globe and Mail*, the *Toronto Star* had 35 relevant articles in the period, *National Post* with 21, *The Ottawa Citizen* and *Le Droit* both with 17, and *La Presse* with eight. Other news media sources did repost content from other places, but not to the same extent that *The Globe and Mail* did. It is interesting that the French news

media sources had less reports on GC cyber security, but there were higher levels of Quebec provincial-level articles in the domain than the English news media had for any province or territory. How then did the GC stories play out in news media perceptions?

Major Themes from the 2018 Period

During the 2018 period there were several key themes that stood out. Notably, the Huawei 5G story was central to 38.5% of the articles reviewed. Articles did span the whole period but intensified in proportion in December when Ms. Meng was arrested and the two Canadian Michaels subsequently detained (Agence France-Presse, 2021). Articles that mentioned Huawei 5G without a cyber security vantage or focused on other forms of Chinese foreign interference were not included in that count. The five next most referenced themes included Chinese cyber hacking and espionage (7.8%), election interference cyber security risks (7.8%), public attribution of Russian cyber attacks (4.7%), Canadian businesses impacted by cyber attacks (4.2%), and Statistics Canada's data collection of personal banking information with potential exposure to hacking (3.6%).

Headlines, Abstracts, and Body Text Perceptions

Starkly, 83.3% of headlines across the articles were neutral (as shown in Figure 2 below). This indicates that the news media generally did not use headlines to present perceptions of the GC in cyber security in this period. Notably, when they did choose to do so it was more often negative than positive or ambiguous by over five times each.

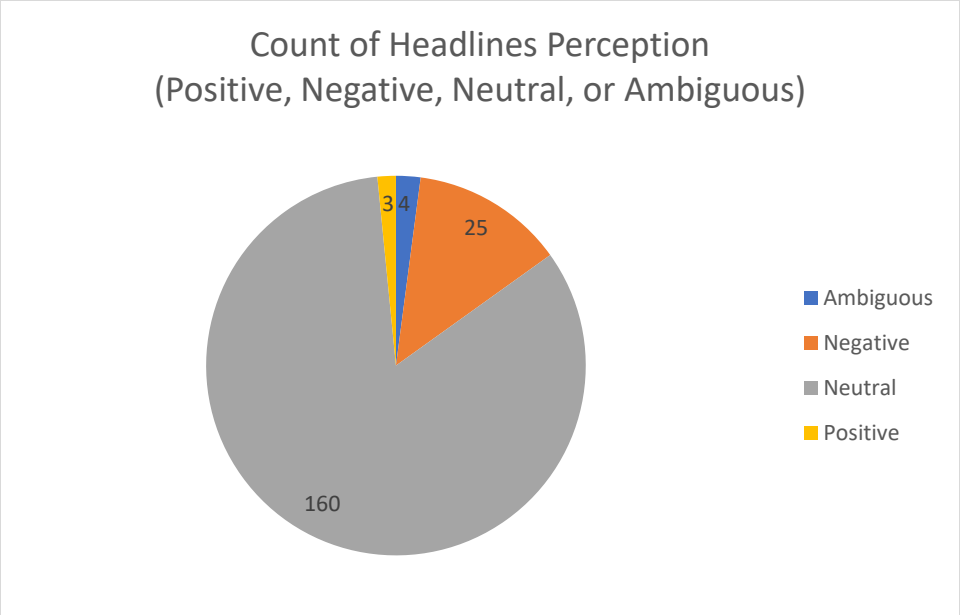

Figure 2: 2018 Count of Headlines Perceptions

Eight of the negative headlines were critical of the GC approach to the Huawei 5G decision-making (Chiu & Grauer, Federal government under fire for Canada's Huawei ties, 2018) (Green, 2018) (Chase & Fife, U.S. senators urge Trudeau to block Huawei from 5G; In letter to PM, two senior committee members warn inadequate safety measures put Canadian national security and 'Five Eyes' joint intelligence, 2018) (Fife & Chase, U.S. intelligence officials question Canada's ability to test China's Huawei for security breaches; Senior officials reportedly laugh at declaration that Canada possesses sufficient safeguards to address risks posed by telecom giant, 2018) (Fife & Chase, Five Eyes spy chiefs warned Trudeau twice on Huawei risk, 2018) (Fife & Chase, Five Eyes spy chiefs warned Trudeau twice about Huawei national-security risk; Sources said the spy chiefs stressed that their countries cannot become dependent upon Huawei's 5G technology, 2018) (Scholtz, 2018) (Freeze, Cyber czar says Canada has 'layers' to protect against potential Huawei threat, 2018) and three others were skeptical of Canada's approach to China writ large (The Globe and Mail, 2018) (McCall, 2018)

(McKenna, Now is not the time for Canadian businesses to retreat from China, 2018). Four negative headlines were on Statistics Canada's requests for personal banking information with terms like snoopy (Latouche, 2018), privacy watchdog probe (Curry, Privacy watchdog probes Statscan move to collect personal banking data, 2018), and that it must be justified (Curry, Statscan must justify request for personal banking data, former chief says, 2018) (Slobodian, Evening Update: Privacy commissioner probing Statscan over efforts to obtain banking records; Canada's economy grows for seventh straight month; Also: Halifax woman with terminal cancer plans to die tomorrow, saying law is forcing early death on her, 2018).

Only three articles provided positive perceptions of the GC in their headlines. The positive headlines pertained to Canada being prepared for possible Chinese cyber retaliation for the arrest of Ms. Meng (The Globe and Mail (Breaking News), 2018), having Canada united with 50 countries against cyber crime (La Press+, 2018), and Canada remaining a nation of laws (Black, 2018). This implies that the news media is not captured by the government as a promotional apparatus and indeed there is freedom of the press. It could also mean the GC was not leveraging traditional news media effectively to communicate messaging on cyber security efforts as good news stories for the public.

Abstracts did not provide much to work with in this period. Most of the articles did not have abstracts and where they were included in 2018 the content was always neutral. No further inferences were gleaned in abstracts, so analysis moved into the body text.

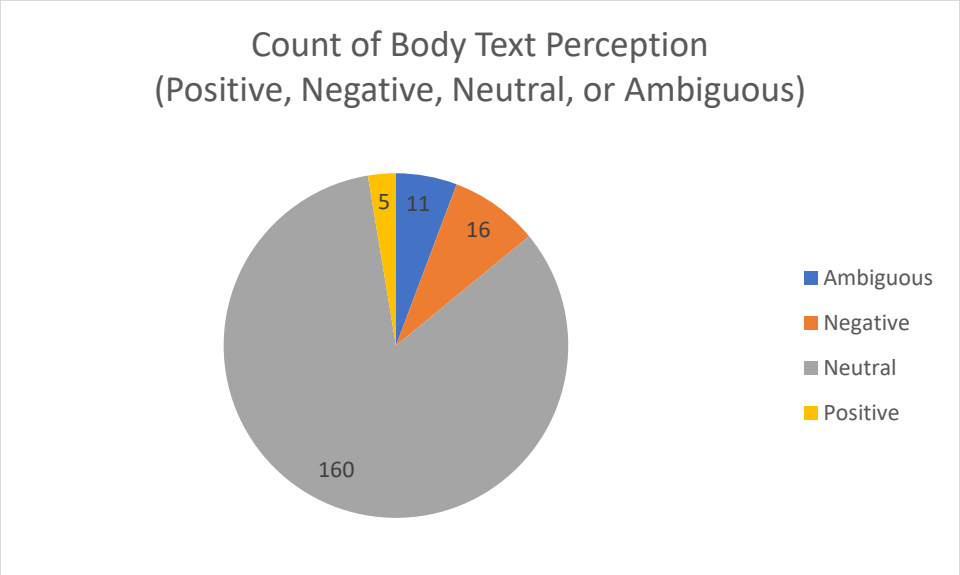

Figure 3: 2018 Count of Body Text Perceptions

The body text was largely neutral at 83.3%. Akin to headlines, there were more negative perceptions (8.3%) than positive (2.6%) or ambiguous (5.7%). Unlike headlines there was more prevalent ambiguousness (at 8.3% over comparable percentage in headlines of 2.1%) and lower negative perceptions (at 8.3% versus 13.0% in headlines). This could indicate some click-bait style headlines being used to draw readers in while the main body content itself is more nuanced by presenting multiple viewpoints without ultimately providing a perception of the GC. Where the body text was ambiguous there were positions posed both in favour of and against the GC's activities in cyber security without a clear victor in the article. That with nuance in headlines and body text negative was the more frequent than positive or ambiguous indicates that the press did provide some level of a challenge function.

Negative perceptions in body text were demonstrated in 16 articles from *The Globe and Mail* (eight), *National Post* (four), *Toronto Star* (three), and *The Ottawa Citizen* (one). *The Globe and Mail* included one article twice on the same day with different headlines,

one that was negative and the other neutral. Both provided contrary opinions to Canada's ability to mitigate the risks associated with Huawei 5G (Fife & Chase, U.S. intelligence officials question Canada's ability to test China's Huawei for security breaches; Senior officials reportedly laugh at declaration that Canada possesses sufficient safeguards to address risks posed by telecom giant, 2018) (Fife & Chase, U.S. security officials question Canada's ability to test Huawei risks, 2018). There were other articles critical of GC's approach to Huawei 5G from the *Toronto Star* (Chiu & Grauer, Federal government under fire for Canada's Huawei ties following arrest in Vancouver, 2018) and *The Globe and Mail* (Chase & Fife, U.S. senators urge Trudeau to block Huawei from 5G; In letter to PM, two senior committee members warn inadequate safety measures put Canadian national security and 'Five Eyes' joint intelligence, 2018) (Chase & Fife, U.S. senators urge Trudeau to block Huawei from 5G, 2018), including one critical of business retreat from China (McKenna, Now is not the time for Canadian businesses to retreat from China; Canada must look past current concerns to protect future growth in mutually beneficial dealings between the two countries, 2018). The articles were predominantly critical of Canada not aligning to some Five Eyes allies' perspectives on banning Huawei from 5G networks or skeptical of GC's ability to test and mitigate related risks.

Other negatively skewed articles related to Canada's geopolitical cyber security posture and trade relations. This includes reliance on the United States (Burney, 2018) and United States-Mexico-Canada Agreement (USMCA) digital and data localization concerns (Mcleod, Data localization fears may be inflated; Usmca, 2018) (Israel & Tribe, 2018). One article was critical of free trade-related negotiations with China calling them

absurd (McCall, 2018). One piece had concerns and negative perspectives on potential Five Eyes 'backdoor' for technology devices raising privacy issues (Thomson, 2018).

There were also negative perspectives on domestic cyber security activities. A few articles dealt with privacy considerations of Statistics Canada's request for personal banking information with concerns for identity theft (Latouche, 2018) (Wells, What identity theft can teach Trudeau, 2018) (Wells, Jennifer Wells: What one unsettling tale of identity theft can teach Justin Trudeau about data privacy, 2018). One article was critical of Canada's anti-spam rules impacting companies whose customers use their products or services maliciously without the company's knowledge indicating that reprimanding them is unfair (Schiestel, 2018). Another piece indicated that many companies were not ready for the new data-breach response rules (Castaldo, Many companies not ready for new data-breach response rules, experts say, 2018). These new data-breach response rules were important for GC's ability to act on broadscale cyber security threats faced by Canadian businesses and engendering stakeholder buy-in is critical to success.

Five articles contained positive perspectives of the GC in their body text. Two came from the *National Post* and one from *The Ottawa Citizen* was an apparent repost from a *National Post* article under the same authors and headline. Two others came from *The Globe and Mail*. The duplicate article pertained to election meddling for the 2019 election and included supportive comments on the GC's activities including a quote from the North Atlantic Treaty Organization's Deputy-Secretary General about how Canada is a great example in "pushing back against disinformation" amongst other supportive points (MacDonald & Doucette, Voters warned of meddling in 2019 election; Russian efforts cyber-security plan touted by defence minister, 2018) (MacDonald & Doucette, Voters

warned of meddling in 2019 election; Russian efforts cyber-security plan touted by defence minister, 2018). Three positive body text perceptions pertained to Huawei 5G. One from the *National Post* included positive comments regarding the GC's criminal justice system dealings with Ms. Meng (Black, 2018), which did not include GC cyber security activities or programming commentary. *The Globe and Mail* articles had opposing views with regards to Canadian relations with China. One highlighted the GC's preparedness for potential Chinese retaliation (The Globe and Mail (Breaking News), 2018) while the other supported the GC Huawei 5G approach since "Huawei leads the world in 5G technology and contributes much to our country" (House, It's About Competition, 2018). There were mixed opinions in the press about the GC approach to Huawei since most of the negative articles were on this while positive stories also made the press. This indicates that there is freedom of the press from political capture and willingness to provide a challenge function.

Inclusion of GC in Articles

Speaking Points and Content

Most articles from 2018 included GC speaking points or content (73.4%). This could indicate that media activity was led by what the GC was publicizing itself rather than journalist-driven initiatives using methods like Access to Information / Privacy requests or other lines of enquiry. This may be indicative of a public dissemination model of government-media relations. However, it is possible that behind the scenes questions from news media may have been a part of the GC providing public content, which would indicate a two-way asymmetrical model with the GC having greater knowledge regarding their own cyber security activities. There are interesting insights from what was included.

The most prevalent narrative throughout was Canada's position on Huawei 5G and the GC's associated cyber security posture. It was no surprise that the GC's communications in this area had a heavy presence in news media. In 2018, 53 articles (38.1%) included speaking points on these issues from Prime Minister Justin Trudeau, Greta Bossenmaier (Trudeau's then National Security Advisor), then Head of CCCS Scott Jones, CSE spokesman Ryan Foreman, Head of CSIS David Vigneault, CSIS' then Chief Information Officer Tahera Mufti, then Public Safety Minister Ralph Goodale, and/or Global Affairs Canada's spokesperson Stefano Maro or public facing content like CCCS security testing of telecommunications products (for citations please refer to Appendix C – 2018 Citations for GC Speaking Points or Content on the Canadian Position on Huawei 5G and Canada's Cyber Security Posture). As an issue raised by Five Eyes allies it was important to get messaging out to substantiate the GC's decision-making processes for them and the Canadian public trust.

Elections interference was a theme across 13 articles (9.4%). GC content included Defence Minister Harjit Sajjan's warnings and speaking points around impact of fake news for the coming election (The Canadian Press, 2018) (MacDonald & Doucette, 2018) (MacDonald & Doucette, Élections fédérales: Ottawa, 2018) (MacDonald & Doucette, Voters warned of meddling in 2019 election; Russian efforts cyber-security plan touted by defence minister, 2018) (MacDonald & Doucette, Voters warned of meddling in 2019 election; Russian efforts cyber-security plan touted by defence minister, 2018). Other articles highlighted Elections Canada's speaking points on shoring up cyber security and public awareness campaigns (The Globe and Mail, 2018) (The Globe and Mail (Breaking News), 2018), speaking points from then Head of CCCS Scott Jones on monitoring for

elections meddling (Boutilier, Bracing for election meddling; Provinces get primer from national spy group, 2018) (Boutilier, Feds brief provinces on election interference threat, 2018), the Head of CSIS David Vigneault's speaking points on state-sponsored espionage, dual-use technologies, and federal elections interference (Campion-Smith, 2018) (Campion, Growing threat of espionage threatens Canada's economic interests, spy agency head warns, 2018), as well as Liberal MP Karina Gould's speaking points on it being virtually impossible to prevent foreign interference during elections (Boutilier, 'Virtually impossible' to prevent foreign meddling in 2019 election, Karina Gould says, 2018) (Boutilier, Election meddling a threat, Ottawa says; 'Virtually impossible' to prevent foreign interests from spreading misinformation, minister warns, 2018).

The GC's condemnation of Chinese state-sponsored hacking spanned 11 articles (7.9%) (Hannay & James, Politics Briefing: LNG project good for business, but may threaten environment; Also: Trudeau says Canada-China trade won't be stopped by USMCA clause, 2018) (Snider, 2018) (Hannay, Politics Briefing: Trudeau's carbon-tax fight is getting more complicated; Also: Canada condemns Chinese hacking, 2018) (Chase S. , Canada joins U.S., U.K. in calling out China for state-sponsored hacking campaign; The move comes as Canada is weighing whether to allow Huawei Technologies to supply gear for next-generation 5G mobile networks, 2018) (Blackley, 2018) (Slobodian, Evening Update: Third Canadian detained in China for working illegally, Beijing says; Ottawa gives Toronto $7-million to combat gangs and guns; Also: Canada can reach Paris emissions target with faster adoption of electric cars, public transit: McKenna, 2018). Five of these had GC speaking points, including CSE's statement supporting United States' allegations against China for cyber hacking as well as then

Public Safety Minister's comment regarding not being aware of Canadian accounts having been impacted (Bronskill, Canada among hacking targets; Two Chinese citizens charged with waging a campaign to steal data, 2018) (La Presse Canadienne, 2018), CSIS points that Canadian research was "of interest to foreign states," whose exploitation of such work posed potential harm to "Canada's national interests" were covered (Ligeti, Morning Update: A last-minute deal to save Calgary's Olympic bid; Chinese firm diverted web traffic; Also: Canadian hospitals are reporting a spike in a rare syndrome resembling polio, 2018). The China Telecom diversion of internet traffic in Canada and the United States story included speaking points from both Prime Minister Justin Trudeau's then National Security Adviser Greta Bossenmaier and Global Affairs Canada spokesperson Stefano Maron (Fife & Chase, China Telecom diverted online traffic, report says, 2018). Other condemnation of Chinese state-sponsored hacking included former Chief of Defence Staff General John Vance's speaking points on geopolitical relationships with China and CSE statements indicating that China was likely behind hacking of corporate systems since 2016 (Campion, Canadian air force aircraft harassed by Chinese during patrols off North Korea, 2018). Given the extent of this activity there was a clear cause for concern of Chinese interference in other areas like 5G networks.

Canada's public attribution of Russian state-sponsored cyber hacking was a theme across nine articles (6.5%), which included attacks on a range of organizations like the Organization for the Prohibition of Chemical Weapons in the Netherlands and the Canadian headquarters of the World Anti-Doping Agency (National Post News Services, 2018) (Slobodian, Evening Update: Canada, allies rebuke Russia over alleged hacking; Quebec Liberal leader Couillard retires from politics; Also: U.S. not invited to Canada's

save-the-WTO summit of 'like-minded' countries, 2018) (Arthur, Faster, stronger and ... spy-er? RUSSIA, 2018) (Arthur, Bruce Arthur: Russian hackers have become the spies who love, 2018) (Cook, 2018). Some others had speaking points from then Foreign Affairs Minister Chrystia Freeland's office that Canada was not expelling Russian citizens associated to the public statement for Russian attribution (Chase S. , Canada joins censure of Russian hacking, 2018) (Chase S. , Canada, Western allies rebuke Russia over alleged global, 2018) (Blanchfield, Canada blames Russia for hacks; NATO countries claim cyberattack targeted anti-doping agency, 2018) (Thibodeau, 2018) as the Dutch had done with four Russian intelligence officers. The Global Affairs Canada statement indicated that these attacks "underscore the Russian government's disregard for the rules-based international order, international law and established norms" (Blanchfield, Canada blames Russia for hacks; NATO countries claim cyberattack targeted anti-doping agency, 2018).

Policies and Programs

Across the 2018 articles reviewed 38.0% did demonstrate awareness of GC policies and programs. However, only two articles provided links to GC sources and both provided contact information for the Canadian Anti-Fraud Centre for victim reporting (Donovan, RCMP dives into phishing probe; In effort to crack down on cybercrime, asking victims to report cases, 2018) (Donovan, Have you been hacked or phished? The Mounties want to know, 2018). This was an important communique to the public as the GC is dependent upon reporting for investigations into cyber threat actors. Other public-facing resources developed for Canadians and businesses like CSE's Get Cyber Safe intended to improve Canada's overall cyber resilience were not covered in this period,

despite being launched in 2011 (Get Cyber Safe, 2021). This could reduce uptake and therefore challenge the GC's ability to protect the public from malicious cyber activity. The lack of coverage is counter a complete dissemination of information model since these are important communications for building public cyber resilience that CSE actively promoted on public-facing GC sites. Perhaps stories were not picked due to a lack of public interest in cyber security and/or that there were more politicized items dominating the press agenda with finite resources.

41 articles (34.7% of those that pertained to GC policy and programs) related to Huawei 5G including the ongoing cyber security review and existing testing facilities for telecommunications technologies backdoors (for citations please refer to Appendix D – 2018 Citations for GC Policy and Programs related to Huawei 5G Including the Cyber Security Review and Testing Facilities for Telecommunications Technologies Backdoors). These were important messages for the GC to publicize as they were being critiqued for not banning Huawei from 5G. For public trust and allied relationships hearing that there was an ongoing cyber security review as well as testing for backdoors gave some peace of mind that the GC understood and were analyzing the risks.

The GC Digital Privacy Act was referenced in eight articles including the new data breach response rules, which some thought were not strong enough while others warned companies may not be ready for them (Mcleod, New data breach rules not strong enough, critics argue, 2018) (Mcleod, New rules for data breach don't go far enough, critics warn, 2018) (Paddon, 2018) (Brearton & Calleja, 2018) (Calleja & Brearton, 2018) (Castaldo, Many companies not ready for new data-breach response rules, experts say, 2018) (Carmichael & Ahmad, Cybersecurity breaches will soon reverberate all the way up to the

board level; Canada's new mandatory data-breach notification rule means boards can no longer afford to be deferential toward cyberattacks, 2018) (Carmichael & Ahmad, Cybersecurity issues will soon reverberate all the way up to the board level, 2018). This had visibility as an area of public interest impacting individual privacy and business requirements with new breach reporting obligations, resulting in critical perspectives from both sides on the matter. The press was free to critique the GC approach, while still disseminating GC information on the mandatory data-breach notification rule.

Statistics Canada's activities were referenced in 12 articles. The first six articles mentioned or quoted the Statistics Canada survey: cyber attacks on businesses providing some key results and analysis as presentation of facts (Reynolds, Hackers hit more than 1 in five firms in 2017: StatCan poll, 2018) (La Presse canadienne, 2018) (O'Kruk, 2018) (Campion-Smith, 2018) (Campion, Growing threat of espionage threatens Canada's economic interests, spy agency head warns, 2018) (Reynolds, Hackers hit one firm in five in 2017: StatCan; Cyber-Security, 2018). Statistics Canada's request for personal banking information and the Privacy Commissioner's pursuant investigation was also referenced in six pieces (Wells, What identity theft can teach Trudeau, 2018) (Wells, Jennifer Wells: What one unsettling tale of identity theft can teach Justin Trudeau about data privacy, 2018) (Solbodian, 2018) (Curry, Privacy watchdog probes Statscan move to collect personal banking data, 2018) (Krol, 2018) (Curry, Statscan must justify request for personal banking data, former chief says, 2018). In many of the articles on the request and investigation the Office of the Privacy Commissioner's investigation was presented positively with Statistics Canada critiqued for overreach. Privacy was a concern for Canadians and common theme in this period of news media sources.

Other themes were referenced in three articles each. CRTC's Anti-Spam Law applied fines to two companies (National Post, 2018) (The Canadian Press, 2018) (The Canadian Press, 2018). CSE monitored for potential online disinformation campaigns or hacking attempts aimed at compromising the election (Boutilier, Election meddling a threat, Ottawa says; 'Virtually impossible' to prevent foreign interests from spreading misinformation, minister warns, 2018) (Boutilier, 'Virtually impossible' to prevent foreign meddling in 2019 election, Karina Gould says, 2018) (The Globe and Mail, 2018). Digital policy in trade relations under the new USCMA including data localization considerations were discussed (Mcleod, Data localization fears may be inflated; Usmca, 2018) (Mcleod, Concerns Over Data Localization Ban In Usmca Could Be Overblown; New trade deal may have provision that allows for carveout, James McLeod writes, 2018) (Israel & Tribe, 2018). Lastly, Canada becoming a signatory to the Paris Call to Action on cybercrime was detailed (La Press+, 2018) (La Presse canadienne, 2018) (Associated Press, 2018).

Departments or Agencies

2018 articles referenced 27 departments and agencies as detailed in Table 1 below, including Crown corporations and Canada as a state actor. There were 213 unique mentions – most were neutral. Only nine departments or agencies were referenced over four times, meaning that 18 had less than a handful of mentions. With the breadth of accountabilities detailed in the Background Literature Review it was clear that most work was not captured. The three most referenced departments and agencies were CSE (21.1%), CCCS (17.8%), and the RCMP (11.7%). Interestingly, that CSE and component CCCS were the most referenced entities as the technical authority and Public Safety Canada as the policy authority for NCSS was only mentioned twice. The Minister of Public

Safety was referenced or quoted six times so their direction was being provided while perhaps not naming the organization itself. Of the articles where there was some sway one article was positive, four were ambiguous, and 15 were negative. This indicates that the press was generally neutral when reporting on departments and agencies but slanted to the negative where they did take a stance. In terms of government-media relations this implies that while seeming to be source driven by the extent of speaking points and content inclusion (one-way), that the publicity model does not fit as there is no hype or spin, but the dissemination could fit better.

Table 1: 2018 Counts of Departments and Agencies Mentioned

Department or Agency	Count of Mentions
Communications Security Establishment	45
Canadian Centre for Cyber Security	38
Royal Canadian Mounted Police	25
Canadian Security Intelligence Service	15
Statistics Canada	14
Global Affairs Canada	12
Office of the Privacy Commissioner	11
Canada as a state actor	9
Canadian Radio-television and Telecommunications	9
Elections Canada	4
Senate of Canada	4
National Research Council	4
Justice Canada	2
Destination Canada	2
Office of the Commissioner of Lobbying	2
Public Safety Canada	2
Natural Sciences and Engineering Research Council	2
House of Commons	2
Bank of Canada	2
Immigration, Refugees and Citizenship Canada	2
Department of National Defence / Canadian Armed Forces	1
Canadian Internet Registration Authority	1

Department or Agency	Count of Mentions
Treasury Board of Canada Secretariat	1
Sustainable Development Canada	1
Canadian Anti-Fraud Centre	1
Canada Border Services Agency	1
Innovation, Science and Economic Development Canada	1

GC puff pieces were not evidenced in either period analyzed, but the CRTC was framed positively in 2018 for their ruling on an industry proposal to fight pirated content. The website-blocking regime proposed was rejected by the CRTC and the author commended CRTC in this ruling as they did not have the jurisdiction to implement the proposal and further that it conflicted with copyright law (Jackson, Website-blocking plan to fight online piracy rejected by CRTC, 2018). The article provided several favourable perspectives on the CRTC's ruling finding it the appropriate approach.

Of the four ambiguous perspectives on departments and agencies, three pertained to Statistics Canada's request for personal banking information which was under review with the Office of the Privacy Commissioner (Krol, 2018) (Curry, Privacy watchdog probes Statscan move to collect personal banking data, 2018) (Curry, Statscan must justify request for personal banking data, former chief says, 2018). These articles provided pros and cons to the Statistics Canada request without developing a favourable or negative point of view. Perhaps this was because there was already an ongoing review with the Office of the Privacy Commissioner, which was framed neutrally. The other ambiguously framed department was Justice Canada regarding the arrest of Ms. Meng providing concerns of economic costs and retaliation as well as positions of Canada needing to stand firm (Blanchfield, Business facing risk of retaliation; ANALYSTS, 2018).

From the 15 negatively skewed articles, there were five areas where the GC was critiqued as detailed in analysis above: Huawei 5G, Statistics Canda's request for personal banking information, data localization and policies in USMCA, concerns with data breach rules, and there were critiques of Destination Canada's suspension of advertising in China. Four pieces were critical of the CCCS' stance at the time that Huawei would not be banned from 5G networks. They each urged the GC to consider banning Huawei, when then Head of the CCCS had concerns over blocking Huawei given limited suppliers potentially putting Canada at risk (Chase & Fife, U.S. senators urge Trudeau to block Huawei from 5G, 2018) (Chase & Fife, U.S. senators urge Trudeau to block Huawei from 5G; In letter to PM, two senior committee members warn inadequate safety measures put Canadian national security and 'Five Eyes' joint intelligence, 2018) (Fife & Chase, U.S. intelligence officials question Canada's ability to test China's Huawei for security breaches; Senior officials reportedly laugh at declaration that Canada possesses sufficient safeguards to address risks posed by telecom giant, 2018) (Fife & Chase, U.S. security officials question Canada's ability to test Huawei risks, 2018). Telecommunications resilience with failover protocols remains a relevant concern with limits to suppliers or technologies as evidenced by the recent Rogers outage and its impacts on GC operations. Statistics Canada's request for personal banking information was critiqued in three pieces with concerns for identity theft and claiming it was an overreach (Latouche, 2018) (Wells, What identity theft can teach Trudeau, 2018) (Wells, Jennifer Wells: What one unsettling tale of identity theft can teach Justin Trudeau about data privacy, 2018). Canada as a state actor was negatively framed in three articles on digital and data elements. One was critical of the blanket ban on data localization policies

(Mcleod, Data localization fears may be inflated; Usmca, 2018). Another indicated that the "deal demonstrates lack of foresight" and serves to "sign away Canada's digital future" (Israel & Tribe, 2018). The last indicated that Canada was not prepared for cyberattacks and had a weak cyber security posture (Burney, 2018). Data breach rules under the new section of the Personal Information Protection and Electronic Documents Act were the focus of three articles. Two critiqued the data breach rules for not going far enough to protect the privacy of citizens, including perspectives from then Privacy Commissioner Daniel Therrien (Mcleod, New data breach rules not strong enough, critics argue, 2018) (Mcleod, New rules for data breach don't go far enough, critics warn, 2018). The other indicated that many companies were not prepared for the new data-breach response rules (Castaldo, Many companies not ready for new data-breach response rules, experts say, 2018). Two articles had negative slants on Destination Canada's suspending advertising in China to protect the tourism brand stating that "it is not the time for Canadian businesses to retreat from China" (McKenna, Now is not the time for Canadian businesses to retreat from China; Canada must look past current concerns to protect future growth in mutually beneficial dealings between the two countries, 2018) (McKenna, Now is not the time for Canadian businesses to retreat from China, 2018).

Political Figures

Many political figures were named across in the 2018 period[1]. As with other fields of inquiry, neutral was the most frequent approach. 12.5% of articles included some nuance with four ambiguous, three positive, and three negative representations. With less than a handful of pieces including nuance on political figures there are further indications

[1] For a complete set of political figures named please refer to Appendix E - Database of Articles Consulted for a link to the database of records and review tab 2018's column X.

of information dissemination via press reporting since many of the political figures referenced had speaking points included in articles as evidenced above. This could also indicate a two-way model that is asymmetric, since the communicators of GC speaking points and content certainly have greater power for intelligence into GC activities or one that is symmetric if public opinion was leveraged to develop communications. Two-way models could not be completely gleaned without access to internal documentation, which was out of scope.

The ambiguously framed political figure across each of those articles was Prime Minister Justin Trudeau regarding Canada's continued involvement with Huawei providing pros and cons on that decision without support or reprimand of approach (Chiu & Grauer, Federal government under fire for Canada's Huawei ties following arrest in Vancouver, 2018) (Chiu & Grauer, Federal government under fire for Canada's Huawei ties, 2018) (Campion, Growing threat of espionage threatens Canada's economic interests, spy agency head warns, 2018) (Fife & Chase, China Telecom diverted internet traffic in U.S. and Canada, report finds; Cybersecurity researchers say state-owned firm has shunted data through legal access points in North America in an effort to steal intellectual property, 2018).

Three articles on Huawei 5G had negative views on the GC's approach which ultimately laid blame on Prime Minister Justin Trudeau with a heavier focus on then opposition leader Andrew Scheer's position on Huawei 5G that the Prime Minister was dragging out the decision (Fife & Chase, Huawei chairman challenges security risk concerns, demands proof that tech giant is a pawn of Beijing; Huawei chairman warned that banning Huawei from supplying next-generation 5G mobile technology to Western

countries would raise costs to consumers and s, 2018) (Ligeti, Morning Update: Charges stayed in major B.C. money-laundering case; another Five Eyes ally bars Huawei from 5G;, 2018) (Proceviat, 2018). These articles urged action and raised allied warnings about associated risks for Chinese cyber interference in 5G, which critiqued the GC approach.

Three pieces portrayed political figures positively with single mentions each, indicating a lack of political promotion represented in the media. Daniel Therrien then Canada's Privacy Commissioner's perspectives on the data breach notification rule were included in one article. However, while favourable of his speaking points they are not as favourable of the GC approach because his points indicate that the GC was not going far enough. They include his critiques about the GC not having regulatory authority to order companies to comply as is the case in Europe and the United States (Mcleod, New data breach rules not strong enough, critics argue, 2018). Another piece was favourable of Harjit Sajjan, then Canada's Defence Minister, for warnings to voters about elections meddling targeting via cyber attacks and fake news with Russia stepping up in undermining western democracies (MacDonald & Doucette, Voters warned of meddling in 2019 election; Russian efforts cyber-security plan touted by defence minister, 2018). The last piece provided favourable representation of Manon Gaudet, head of the cyber security research group for the National Research Council about her messaging on needing to adapt while bringing new technologies into critical infrastructures, which pose security challenges (Paquette, 2018).

2021 Summary

This section summarizes the 2021 news media from 119 unique articles between July – December 2021 (62.0% of the number of articles from the 2018 period). The counts

were closer across sources, except that *The Globe and Mail* was over four times the next closest source (*National Post*) per Figure 4 below. As mentioned above, there are reporting practices from *The Globe and Mail* that drive the higher article count like summary wrap-ups and reposting under different titles or versions. Re-use of stories could be indicative of a symbiotic relationship between the GC and media whereby journalists were dependent upon them for consistent and reliable content.

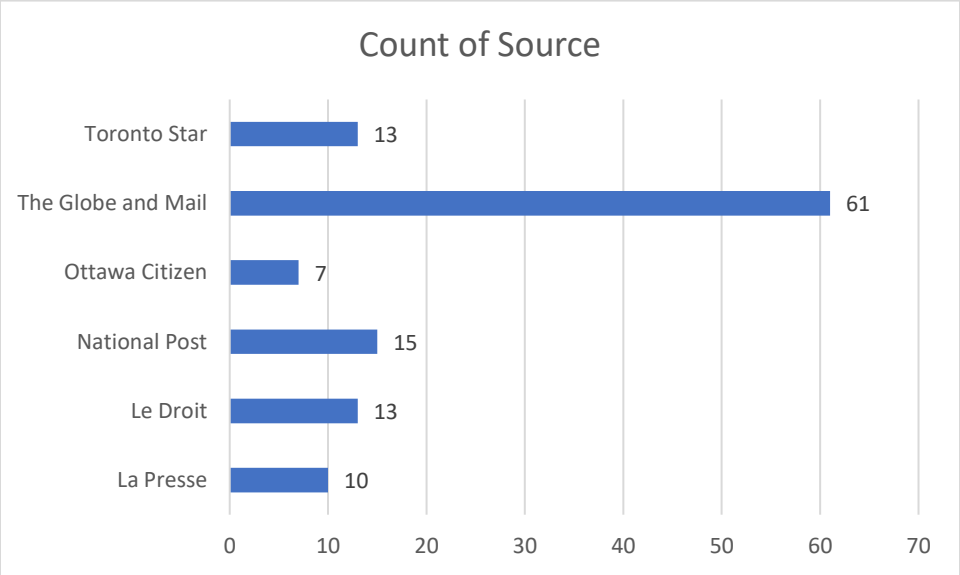

Figure 4: 2021 Count of Source References

GC cyber security was less prominent in news media during the 2021 period by sheer article counts, but there were many other things on the radar. The count of articles from each source dropped from 2018 except for *La Presse* (up to ten from eight). To be fair there were major other events that required public visibility like responses to different permutations of the COVID-19 pandemic (Delta then Omicron) (Pelley, 2021) and a federal election (Elections Canada, 2021) with finite journalistic resources in traditional news media. Moreover, under the new hybrid work models necessitated during the COVID-19 pandemic there could have been strains on traditional lines of communication

between the GC and news media in this period reducing access and posing challenges to get the GC narrative in the press. Another rationale for lower coverage in 2021 could be that the GC was just doing so well in cyber security behind the scenes that raised less flags to the press. Alternatively, the GC could have been choosing to disseminate less information on cyber security to not overwhelm the public that was being flooded with different information regarding public health consistently across this period on vaccines and COVID-19 as well as providing sufficient space for free press on the election to enable educated voting. The latter would indicate a one-way dissemination model and perhaps it was a mix of all these factors.

Major Themes from the 2021 Period

Increasingly activity had been driven online during the COVID-19 pandemic and the public faced some proximate threats that amplified cyber crime as a theme in 2021. Ransomware alone was the most common theme across 15.1% of articles reviewed, and particularly with regards to critical services at 6.7%, which came under attack, including health care facilities already overburdened combatting the COVID-19 pandemic (Freeze, Newfoundland cyberattack an 'alarm bell' for Canada, 2021). Another 5% of articles had cyber crime themes of gun trafficking, Canada's cyber security posture more broadly, RCMP's arrest of Marco Pizzi, or protecting youth and other vulnerable populations from exploitation. This could indicate a dissemination model based on the proximate concerns of the public.

The Huawei 5G storyline continued in 2021 across 13.4% of articles as the second-most referenced (at less than a third of the articles from 2018). Chinese foreign interference, including hacking of Microsoft email servers was the third most common

theme (12.6%), indicating that China remained a prime threat. These GC communications were important to Five Eyes allies and public trust while the Huawei 5G decision was still ongoing, which is indicative of a dissemination model.

Other areas received some attention, included the AUKUS trilateral security pact between Australia, the United Kingdom, and the United States as well as the Canada Pension Plan's cyber security technology investment choice received 5.0% coverage each. These were followed by stories on the Governor-General's office network as a victim to 'unauthorized access' (4.2%), deterring Russian aggression (3.4%), quantum computing (3.4%), cyber security related election interference (2.5%), and the Log4Shell zero-day vulnerability in Log4j (2.5%). This indicates that despite lower coverage on GC cyber security activities in this period, some beyond the highly politicized ones mentioned above were still picked up as matters in the public interest.

Headlines, Abstracts, and Body Text Perceptions

Most headlines in 2021 were neutral (79.0%), followed by negative (18.5%), ambiguous (1.8%), and positive (0.8%) (see Figure 5 below). While ambiguous remained less than a quarter percentage point different than 2018, negative increased by over 5.0% from 13.0%, and positive was down from 2.6% in 2018 to just under a third of that indicating an increased criticality of the GC. In fact, only one headline skewed positive. Negative in 2021 was over seven times positive and ambiguous combined versus over five times each of those individually in 2018, indicating a higher tendency for the press to be critical in headlines, but whether that carries through body text or implies click bait techniques is evaluated below.

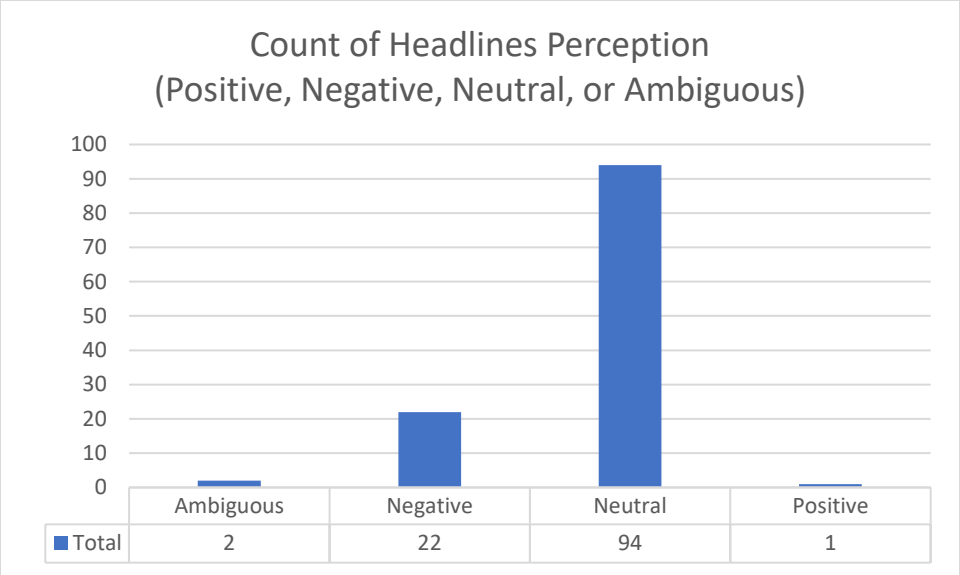

Figure 5: 2021 Count of Headlines Perceptions

Abstracts in French sources from 2021 provided some nuances. Four of 12 articles with abstracts were negative while the rest were neutral. The negative abstracts all related to cyber crime, including needing to prove strong leadership in combatting trafficking firearms, including associated cyber crime (Gagnon C.-A. , Trafic d'armes à feu: le fédéral doit, 2021) (Gagnon C.-A. , Lutte au trafic des armes à feu: le fédéral doit faire preuve d'un «leadership fort», selon les directeurs de police du Québec, 2021), needing a maximum alert with pirates on the horizon (Grammond, Un ministre contre les pirates, 2021), and cyber crime risks facing the GC (Miró, 2021). This shows there was critical pressure on the GC to address cyber crime and communicate this to the public.

In 2021 83.2% of articles were neutral in their body text's content, 5.8% were ambiguous, and 10.9% swayed negatively for the GC as detailed in Figure 6 below.

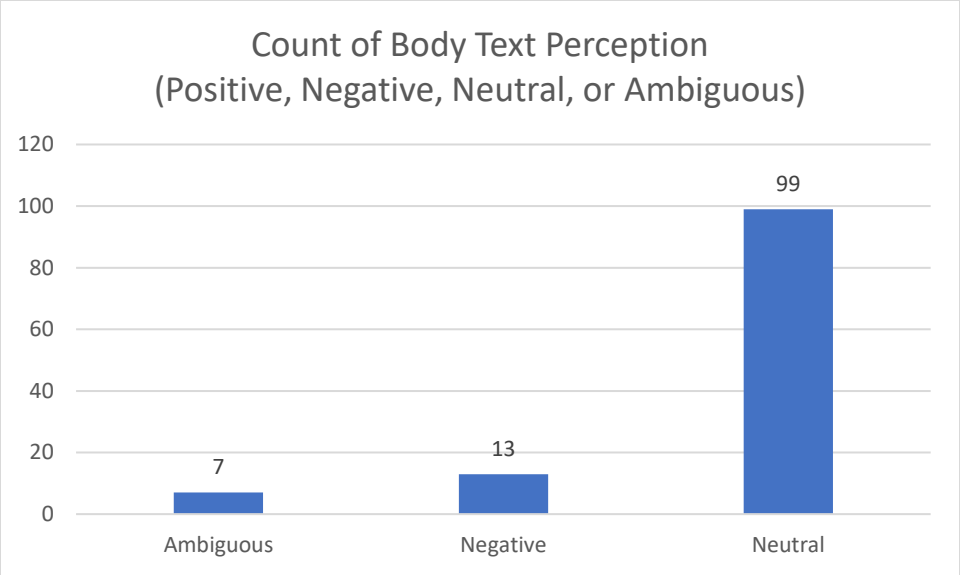

Figure 6: 2021 Count of Body Text Perceptions

Three articles with ambiguous body texts highlighted the risks of why Huawei should be banned, but stated that the GC's approach was still to be determined and were not outright critical that it had not been yet (Karadeglija, Banning Huawei a 'no-brainer' , say analysts; Would be bold stroke but strong message to china and our allies, 2021) (Chase S. , Former Australian PM Malcolm Turnbull says Huawei 5G would leave Canada's networks vulnerable to China, 2021) (Chase S. , Former Australian PM Malcolm Turnbull says Huawei 5G would leave Canada's networks vulnerable to China, 2021). One ambiguous article was on GC security policy writ large, discussing interlinkages between domains needing to be treated as strategically connected but did not indicate that the GC was not planning this approach (Shull, 2021). Another was on AUKUS indicating GC areas of weakness that may have been reasons why Canada was not included in the alliance, but also indicated that it was unclear whether Canada would even want to join such an alliance on nuclear technologies (Carvin & Juneau, 2021) so it was not necessarily negative. Another piece on GC's China policy stated positions from

multiple political parties, some of which were critical of the GC, but without a clear slant in any direction (Glavin, A giant panda in the room; Liberals can't bear to talk about China, 2021). The last ambiguous body text urged for cyber security investments in health care institutions. While it did not outright criticize the GC it called upon both federal and provincial governments dedicate new funding for cyber security capacity (Holland, 2021). This shows more themes of public concerns in news media rather than indicating a model.

Of articles with a slant in their body text, more tilted negatively towards the GC (13), which almost always came in repeat publications (aside from two). Three pieces were critical of the GC's approach to ransomware being reactive (Grammond, Un ministre contre les pirates, 2021), not doing enough, and it not being "even remotely on the radar" (Castaldo, Under Attack, 2021) (Castaldo, Locked out: The growing risk of ransomware hackers has governments, insurers and cybersecurity experts scrambling, 2021). The last two articles cited were published on the same day, in *The Globe and Mail*, by the same author, but with different titles. Another two articles published on the same day, by the same author, under different titles in *The Globe and Mail* critiqued the GC's lagging policy on banning Huawei (Trichur, Canada needs a proper technology security strategy. Banning Huawei from 5G should be the first step, 2021) (Trichur, Banning Huawei from 5G should be first step in assuring security, 2021). Two similar pieces published by the same authors on different dates in the *Toronto Star* were critical of Canada Border Services Agency's use of AI facial recognition technology to screen against 5,000 deportees considering it to be a human rights violation (Mateo & Bhatia, Facial-recognition surveillance threatens our rights, 2021) (Mateo & Bhatia, Reports find that federal government surveillance was again used at Pearson airport, this time through

facial recognition. This threatens our human rights, 2021). Two articles by the same author on different dates in *Le Droit* discussed the GC's need to prove strong leadership in gun trafficking, including associated cybercrime (Gagnon C. A., 2021) (Gagnon C.-A. , Lutte au trafic des armes à feu: le fédéral doit faire preuve d'un, 2021). Another two pieces published on the same day, by the same author, under different titles in *The Globe and Mail* were critical of the Canadian Armed Forces overall approach, indicating that they needed to adapt to the modern world, including pandemic, climate change, and other disasters destabilizing the world (Patterson, 'Defence' doesn't fit the job of Canada's military any more. Let's create a Department of National Safety instead, 2021) (Patterson, The Good Fight, 2021). One author was critical of the Natural Sciences and Engineering Research Council's national security risk assessment requirements with concern that they would chill Canadian research (Parsons, 2021). The last piece critiqued the GC's approach to technology policy in geopolitics broadly considering decisions in the domain as siloed and calling for the election cycle to be an opportunity for re-alignment (Dawson & Ouimette, 2021). Most negative body texts were repeat stories indicating that there was not a hesitation to challenge the GC's approach on issues deemed in public interest to promote shifts in policy direction.

Inclusion of GC in Articles

Speaking Points and Content

In 2021, 66.4% of articles included GC speaking points and content (a 10.0% drop from 2018, which could be in part due to the limitations in communications posed in the hybrid work environment under COVID-19 pandemic restrictions). The drop in content could be from other issues taking greater bandwidth like COVID-19 mandates or elements

other than cyber security related to the federal election called and administered within the 2021 period. Elections interference had more coverage in 2018 for the 2019 election; only three articles in 2021 related to elections targeting by foreign actors. These included speaking points and information from a CSE report on the increasing risk of foreign interference in an election during the COVID-19 pandemic and their confidence in Elections Canada (Berthiame, Cyber agency warns foreign ‘actors' pose threat to Canada's next election, 2021) (Berthiame, Cyberagency warns of election targeting, 2021) (Glavin, A giant panda in the room; Liberals can't bear to talk about China, 2021).

A continued thread was the Huawei’s storyline in 2021, but the geopolitical context between Canada and China had shifted in the same timeframe. Ms. Meng’s proceedings completed in the United States and the two Canadian Michaels were returned at the end of 2021. 12 articles included GC speaking points or content related to Huawei. Four articles referenced Prime Minister Justin Trudeau’s statement that Huawei could soon be prohibited (Trichur, Canada needs a proper technology security strategy. Banning Huawei from 5G should be the first step, 2021) (Trichur, Banning Huawei from 5G should be first step in assuring, 2021) (Fife, Federal cabinet will rule soon on whether to ban Huawei from 5G, 2021) (Fife, Federal cabinet will rule soon on whether to ban Huawei from 5G, 2021). Four pieces included CSIS concerns over loss of intellectual property and sensitive technology to countries like China (Chase S. , Former Australian PM Malcolm Turnbull says Huawei 5G would leave Canada's networks vulnerable to China, 2021) (Chase S. , Former Australian PM Malcolm Turnbull says Huawei 5G would leave Canada's networks vulnerable to China, 2021) (Fife, U.S. envoy warns Canadians about China, 2021) (Fife, New U.S. ambassador to Canada says China is greatest threat to democracy, urges

Ottawa to align with U.S. to challenge Beijing, 2021). Content from then Public Safety Minister Bill Blair's briefing notes on 5G were included in two articles, quoting: "[h]owever, in order to leverage this opportunity for economic growth through 5G, the safety and security of the technology must be ensured" (Bronskill, Canada has no choice but to bar Huawei from 5G networks, security experts say, 2021) and "[i]ncidents resulting from the exploitation of vulnerabilities by malicious actors will be more difficult to safeguard against, and could have a broader impact than in previous generations of wireless technology" (Bronskill, Canada has no choice but to bar Huawei from 5G networks, security experts say, 2021). The translated versions of these quotes were included in a French article by the same author (Bronskill, Des experts en sécurité disent que le Canada doit exclure Huawei de, 2021). Innovation Minister François-Philippe Champagne's statement that Canada would only move forward with "trusted partners" related to Huawei was included in another article (Karadeglija, Banning Huawei a 'no-brainer' , say analysts; Would be bold, 2021). This indicates a dissemination model where the GC may have been laying communications as a foundation for the ultimate decision made to ban Huawei shortly thereafter.

Chinese cyber hacking of Microsoft Exchange servers and emails was a common theme in 2021 where GC speaking points and content was included across 13 articles with public attributions. Former Minister of Foreign Affairs Marc Garneau's speaking points were quoted in six articles, including "Canada is confident that the PRC's Ministry of State Security (MSS) is responsible for the widespread compromising of the Exchange servers" (Snyder J. , 2021) (Snyder J. , 2021) (Fife, Canada, allies condemn China for cyberattack on Microsoft, 2021) (Fife, Canada joins allies in denouncing China for global

Microsoft, 2021) and "[t]his activity put several thousand Canadian entities at risk - a risk that persists in some cases even when patches from Microsoft have been applied" (Fife, Canada joins allies in denouncing China for global Microsoft, 2021) (Paez, 2021) (Fife, Canada, allies condemn China for cyberattack on Microsoft, 2021) (Fife, Canada joins allies in denouncing China for global Microsoft, 2021). A joint statement by then Ministers of Defence Harjit Sajjan, Public Safety Bill Blair, and Foreign Affairs Marc Garneau condemning the activity was referenced and quoted in five articles (Berthiaume, Le Canada et des alliés tiennent la Chine responsable d'une cyberattaque massive, 2021) (Boutilier, Canada joins allies in linking China to Microsofthack, 2021) (Boutilier, Canada joins allies in linking China to Microsoft email hack, 2021) (Berthiaume, Front commun de l'Occident pour dénoncer la Chine, 2021) (Berthiaume, Le Canada et des alliés tiennent la Chine responsable d'une cyberattaque massive, 2021). Two articles referenced the joint statement put out by allies "the European Union, the U.K., NATO, Japan, Canada, New Zealand and Australia" that indicated the "attacks include ransomware, data theft and cyberespionage" (Weil, 2021) (Slobodian, Evening Update: Ottawa joins allies in denouncing China for cyberattacks; fully vaccinated Americans can travel to Canada starting Aug. 9, 2021). This is further evidence of the GC communications framework continuing the narrative of China as a threat actor.

Ransomware, particularly regarding critical services, was another key area where GC speaking points and content were consistently included. Some GC accountabilities in cyber security on cyber crime were included in two articles from the same author, on the same day, in *The Globe and Mail*, under different titles. They both provided a statement from a Public Safety spokesperson's email recognizing the growing threat of ransomware

and that they work with multiple organizations including CCCS in this regard. They also included Inspector Daniel Côté from the RCMP's National Cybercrime Coordination Unit's statements about paying ransom contributing to threat actors getting stronger and more efficient as well as reporting any lead could help make linkages between crimes (Castaldo, Under Attack, 2021) (Castaldo, Locked out: The growing risk of ransomware hackers has governments, insurers and cybersecurity experts scrambling, 2021). In terms of the government-media relations model this is indicative of a call for public support in combatting cyber crime.

CSE and CCCS ransomware content was included in seven articles. This included Sami Khoury Head of CCCS' speaking points on the increase of cyber actors that were becoming more sophisticated and "Canada is among the top countries impacted by ransomware" in three of these pieces (Lapierre, 2021) (Robertson, 2021) (Apparlraju, 2021). CSE/CCCS' statements regarding the response to the Newfoundland health system ransomware cyberattack, including email comments from CSE spokesperson Evan Koronewski "we can assure you we are actively engaged with government and non-government partners, sharing cybersecurity advice and guidance, mitigation, and operational updates related to this matter" (Smellie, 2021). One article also referenced the increase in cyber threat related to the COVID-19 pandemic, including ransomware attacks on Canada's front-line healthcare and medical research facilities (Tutton, 2021). A CCCS cyber threat bulletin was quoted in one article: "[t]he COVID-19 pandemic has made organizations like hospitals, governments, and universities more mindful of the risks tied to losing access to their networks and often feeling resigned to pay ransoms. Cybercriminals have taken advantage of this situation by significantly increasing the value

of their ransom demands" (Nardi & Post, Ransomware attacks targeting health, energy sectors; On rise in 2021, 2021). Another piece included CSE/CCCS' content on ransomware attacks in 2021 as cyber crime via malware, including state sponsored attacks by Russia, China, and Iran (Nardi, 235 known ransomware attacks so far in 2021; Canadian centre says most activity unreported, 2021). CCCS statistics on Canadian businesses who have experienced cyber incidents were detailed in another article (Tison, 2021). While there were critiques on GC's approach to cyber crime evidenced above, news media also provided GC's awareness of the threat environment for ransomware, particularly in critical infrastructure, and provided some of their activities in response.

RCMP content was included in six pieces. Two were on the RCMP's announcement of criminal investigation into the Newfoundland health system cyberattack (Freeze, Newfoundland cyberattack an 'alarm bell' for Canada, 2021) (The Canadian Press, 2021) and the RCMP recommendation not to pay ransom but report attacks (Duquette, Ces terrifiants pirates du Web, 2021) (Duquette, Ces terrifiants pirates du Web, 2021). Another provided Canadian Anti-Fraud Centre speaking points on the impact of fraud and cyber crime (Peesker, 2021). The last included RCMP comments on an ongoing investigation stating that no more information would be released as perpetrators can monitor public statements (Gurney, 2021). Each of these are indicative of dissemination.

Five pieces on the AUKUS Security Agreement included GC speaking points or content. Then Minister of Defence Harjit Sajjan's spokesperson Daniel Minden's email statement was included in three pieces by the same author across a two-day span that "Canada continues to work with its Five Eyes partners on defence technology and

research to strengthen our partnership. We will continue to build on existing collaboration with our allies" (Morrow, Canada left out as U.S., U.K., Australia strike deal to counter China, 2021) (Morrow, Canada left out as U.S., U.K., Australia strike deal to counter China, 2021) (Morrow, Canada left out as U.S., U.K., Australia strike deal to counter China, 2021). Prime Minister Justin Trudeau's statement that AUKUS would have no impact on Five Eyes (Hunnicutt, Bose, Brunnstrom, & Packham, 2021) (Hunnicutt, Bose, Brunnstrom, & Packham, 2021) was twice referenced by the same authors on the same day, but in different periodicals under the same title. This is additional evidence that the GC communications on AUKUS were to provide public confidence that the GC's security alliance with Five Eyes despite scrutiny over the Huawei 5G decision.

Four of the 2021 pieces related to North Atlantic Treaty Organization (NATO) speaking points on deterring Russian aggression (Emmot, 2021) (Emmott, 2021) (MacKinnon, Russia's break with NATO heightens fears of military escalation as two sides trade blame, 2021) (MacKinnon, Russia's break with NATO heightens fears of military escalation as two sides trade blame, 2021). Two were published on the same day in two different periodicals but by the same author under the same title. The other two were published under the same title by the same author days apart in the same periodical. These were important messages for the GC to convey for public confidence in Canada's geopolitical position with alliances in cyber security.

The Governor-General's Office's speaking points from Rideau Hall on the 'unauthorized access' to its network were provided in five articles (Trépanier, Rideau Hall fait l'objet d'une enquête de cybersécurité, 2021) (Trépanier, Rideau Hall fait l'objet d'une enquête de cybersécurité, 2021) as well as working with the Office of the Privacy

Commissioner (Patel, Governor General's network hacked, 2021) (Patel, Gov. Gen. Mary Simon's office says its internal network was hacked, 2021) and CCCS (Bailey, Politics Briefing: Governor-General's office investigating internal network breach, 2021) on the enquiry. There were two articles each from the same two authors in the same periodicals a day apart each under different titles. This indicated public disclosure of information on the breach and GC's response, which was considered important enough for repeats.

Then Privacy Commissioner Daniel Therrien's comments that law enforcement using facial recognition technology was akin to a "24/7 line up" that track "individuals outside of the scope of the problem" were included in two articles (Mateo & Bhatia, Facial-recognition surveillance threatens our rights, 2021) (Mateo & Bhatia, Reports find that federal government surveillance was again used at Pearson airport, this time through facial recognition. This threatens our human rights, 2021). This was messaging condemning an ongoing process being used by CBSA in support of Canadians' faith that their privacy was being protected by the GC.

Policies and Programs

Only 32 articles (26.9%) in this period demonstrated awareness of GC policies and programs, which was down from 38.0% in 2018. Four articles discussed GC commitment of funding to Quantum technologies. Three were on commitments for funding to D-Wave for research and development (Silcoff, Once a pioneer, quantum computer developer D-Wave will start making same types of machines as rivals, 2021) (Silcoff, B.C.'s D-Wave broadens focus, 2021) (Silcoff, Once a pioneer, quantum computer developer D-Wave will start making same types of machines as rivals, 2021). These were all in the same periodical, by the same author, across two days, and with the second day having a

different title for one article. The other was on Natural Sciences and Engineering Research Council funding research in quantum communication and quantum cryptography (Champagne, 2021). These could have been GC placed promoting research and development in quantum technologies, which will be incredibly important in the future of cyber security.

The GC evaluation program for telecommunications evaluation for cyber security risks being around since 2013 was included in three articles (Bronskill, Des experts en sécurité disent que le Canada doit exclure Huawei de, 2021) (Bronskill, Canada has no choice but to bar Huawei from 5G networks, security experts say, 2021) (Bronskill, Des experts en sécurité disent que le Canada doit exclure Huawei de, 2021) by the same author in two periodicals (Le Droit two days in a row and The Globe and Mail on the second of those days). This was important because the Huawei 5G decision was still pending during this time and this supported public trust in the decision-making process.

Natural Sciences and Engineering Research Council's national security risk assessment requirements for scholarly research grants were discussed in three articles. One critiqued Canada's ability to be competitive with the new measure (Parsons, 2021). Two also included content from CSIS meeting with and presenting to Canadian research and industry groups on international espionage including AI and quantum computing (Friesen, CSIS warns Canadian universities to be on alert for international espionage, 2021) (Friesen, CSIS warns Canadian universities to be on alert for international espionage, 2021). Both were from the same author in *The Globe and Mail* with the same title on the same day. All three articles came from *The Globe and Mail*, which indicates a willingness to demonstrate both pro and counter GC perspectives.

Canada Border Services Agency's use of AI facial recognition technology against an existing database of 5,000 deportees to have officers divert individuals to secondary inspection was referenced in two pieces with human rights critiques, but they also referenced then Privacy Commissioner Daniel Therrien's comments condemning this activity (Mateo & Bhatia, Facial-recognition surveillance threatens our rights, 2021) (Mateo & Bhatia, Reports find that federal government surveillance was again used at Pearson airport, this time through facial recognition. This threatens our human rights, 2021). These pieces illustrated GC communications to demonstrate their understanding of the issue identified to engender public trust through dissemination of information.

Two articles from the same author under the same title on different days in *The Globe and Mail* referenced the RCMP's wanting to use AI to obtain passwords to decrypt data seized during criminal investigations. The author demonstrated awareness of the possibility for this to be exempt from the Directive on Automated Decision-Making as the Privacy Commissioner had enabled the Department of National Defence to avoid self-assessment rules for a diversity recruitment campaign (O'Kane, RCMP plan to use AI to obtain passwords could threaten privacy rights, 2021). This indicates another example of concern for privacy regarding law enforcement in Canada using emerging technologies and the media raising it to public attention.

Three CCCS items were highlighted in 2021 articles. CCCS' threat monitoring and reporting with a two-year cyber security review in 2016 that had allocated $1 billion in funding was referenced in two pieces where it was indicated that the GC is not doing enough for cyber security (Castaldo, Under Attack, 2021) (Castaldo, Locked out: The growing risk of ransomware hackers has governments, insurers and cybersecurity

experts scrambling, 2021). The Get Cyber Safe Gift Guide was included in two articles (Carrick, This is how much allowance kids are getting these days, 2021) (Carrick, This is how much allowance kids are getting these days, 2021). The CCCS Ransomware Playbook was included in two pieces (Nardi, 235 known ransomware attacks so far in 2021; Canadian centre says most activity unreported, 2021) (Nardi, Ransomware attacks targeting health, energy sectors; On rise in 2021, 2021). In this period the GC was able to get visibility for some of the public-facing tools and resources that the CCCS has developed for businesses and individuals.

Departments or Agencies

Of the 2021 articles reviewed 65.5% referenced departments and agencies including 115 unique mentions. Most perspectives were neutral, two were ambiguous, and seven were negatively skewed (just under half of the negative references from 2018). The total counts for departments and agencies are provided in Table 2 below with nuances on ambiguous or negatively skewed articles. It is interesting that while negative percentages were higher across headlines, abstracts, and body text in this period that specific departments were called out less frequently in this period.

Table 2: 2021 Counts of Departments and Agencies Mentioned

Department or Agency	Count of Mentions
Communications Security Establishment	19
Canadian Centre for Cyber Security	15
Royal Canadian Mounted Police	13
Canada as a state actor	12
Governor-General's Office	8
Canadian Security Intelligence Service	7
Canada Pension Plan Investment Board	5
Department of National Defence / Canadian Armed Forces	4
Natural Sciences and Engineering Research Council	4

Department or Agency	Count of Mentions
Office of the Privacy Commissioner	4
Canada Revenue Agency	3
Public Safety Canada	3
Canada Border Services Agency	2
Elections Canada	2
Global Affairs Canada	2
National Security and Intelligence Review Agency	2
Natural Resources Canada	2
Prime Minister's Office	2
Shared Services Canada	2
Canadian Anti-Fraud Centre	1
National Research Council	1
National Security and Intelligence Committee of Parliamentarians	1
Privy Council Office	1

The two articles that were ambiguous pertained to the RCMP's potential plan to use AI for passwords but did highlight privacy concerns if exempted from the Directive on Automated Decision-Making as an internal service. This initiative was identified by a request for proposal from the GC. The RCMP response to the media enquiry was included, indicating that this was intended for research and development purposes and would be considered in compliance with the Charter of Rights and Freedoms as well as legal or privacy obligations (O'Kane, RCMP plan to use AI to obtain passwords could threaten privacy rights, 2021) (O'Kane, RCMP plan to use AI to obtain passwords could threaten privacy rights, 2021). Both were by the same author in the same periodical using the same title, but on different days. They demonstrate the public and media concern about privacy and law enforcement.

There were four themes in the negative spectrum for departments or agencies. Two were critical of Canada Border Services Agency's use of facial recognition AI

screening against deportees with human rights claims (Mateo & Bhatia, Facial-recognition surveillance threatens our rights, 2021) (Mateo & Bhatia, Reports find that federal government surveillance was again used at Pearson airport, this time through facial recognition. This threatens our human rights, 2021). Two articles indicated that the Department of National Defence / Canadian Armed Forces was ill-fit for current contexts and required strategic and security policy direction in technology and geopolitics (Patterson, 'Defence' doesn't fit the job of Canada's military any more. Let's create a Department of National Safety instead, 2021) (Patterson, The Good Fight, 2021). The GC approach to ransomware broadly was criticized in two pieces, which referenced the Prime Minister's Office, Public Safety Canada, CCCS, and RCMP (Castaldo, Locked out: The growing risk of ransomware hackers has governments, insurers and cybersecurity experts scrambling, 2021) (Castaldo, Under Attack, 2021). Canada was evaluated as not ready with strategic and security policy direction in technology and geopolitics writ large in one piece (Dawson & Ouimette, 2021). News media provided the challenge function in these cases, which indicates a two-way dialogue that is asymmetric as the GC has greater knowledge of internal operations and strategic directions.

Political Figures

During the 2021 period many political figures were named across 43 articles (36.1%)[2]. There were no ambiguous or positively framed political figures, but two articles did have negative perspectives on Prime Minister Justin Trudeau indicating that he had dragged his feet on the Huawei decision (Bronskill, Des experts en sécurité disent que le Canada doit exclure Huawei de, 2021) (Bronskill, Des experts en sécurité disent que le

[2] For a complete set of political figures named please refer to Appendix E - Database of Articles Consulted for a link to the database of records and review tab 2021's column X.

Canada doit exclure Huawei de, 2021). Both were from the same author in the same periodical under the same title, but a day apart. While there was higher negativity across headlines, abstracts, and body text for the GC in different domains there was much less nuance for political figures evidenced (whereas it was 12.5% nuanced across positive, negative, or ambiguous in 2018). This is indicative of a neutral news media that was not actively criticizing politicians in cyber security while they did not hesitate to challenge GC decisions or programming.

Cross-sectional Analysis

Model of Government-Media Relations

Across periods and frames of analysis the majority of news media content was neutral on the GC regarding cyber security. This remained true across headlines, abstracts, body text, and the departments, agencies, or political figures referenced, which indicated that the news media was neither dominated by promotions nor critiques of the GC. When there was a sway, it was more often negative or ambiguous on the GC indicating that there was no GC spin and the publicity model for government-media relations did not apply. Most articles included GC speaking points or content in both periods [2018 (73.4%) and 2021 (66.4%)], which was indicative of a symbiotic relationship between the GC and news media. This could mean that dissemination of information was the appropriate model for GC-media relations for these periods in that symbiotic relationship with the press reliant upon the GC for steady and reliable content.

There was some evidence of two-way communications models throughout, like the press providing a challenge function, but the asymmetrical and symmetrical models could not be fully assessed given the limited access in this research model. The materials

reviewed did not include internal GC documentation on any polling/surveys done nor any subsequent communications plans. Undoubtedly there were areas where the GC carried out public consultations or other forms of outreach for cyber security-related activities, but they are not captured in this research; it was not possible to determine whether this intel was used to develop persuasive messages or rather to build mutual understanding between the GC and various public audiences. The GC was in a asymmetrical power position with regards to knowledge of their own activities and programming. There was no evidence of GC promotional pieces given that most content was neutral and there was a greater tendency for negative than positive when there was sway in pieces, regardless of whether symmetrical or asymmetrical models were in place.

News Media Trends

Media neutrality was an important trend, which could indicate a professional press corps that presented stories in unbiased ways. Alternatively, technical aspects of cyber security might have been considered too complex for traditional media to report on or for the public to engage with. Regardless, the press was neither a pro nor counter government propaganda machine in either period, instead there was free agency. There were largely a core set of authors who covered the same storylines across both periods and often within the same sources. News media learned from one period to the next about cyber risks as evidenced by the intensified focus on privacy with emerging technologies.

The Globe and Mail tended to post the same or similar articles under different titles on the same day or consecutively in both periods. This implied clickbait headlines as often one title was more nuanced accompanied by neutral titled articles that were duplicates or

near replicas in body content. It drove up content numbers but was not indicative that readership on any given issue was higher.

GC Cyber Capabilities

The GC's cyber deterrence approach included both defensive and offensive cyber capabilities, which were treated differently in news media. Defensive strategies were deterrence by denial through securing and safeguarding systems and business processes or deterrence by punishment meaning that the impact of a breach is of such high cost that it deters would be threat actors (Van Wie Davis, 2021). Offensive cyber capabilities conversely are active cyber operations, which Canada was building capabilities in "to conduct active cyber operations focused on external threats to Canada in the context of government-authorized military missions" in alignment with "all applicable domestic and international law, and proven checks and balances such as rules of engagement, targeting and collateral damage assessments" ((DND), 2017). If Canada did participate in offensive cyber operations over these periods, they were not represented in news media. It would not have been prudent for the GC to advertise offensive cyber operations as it could have undermined their intended purpose. The risk being that there is unpredictability and the potential for collateral damage in using cyber weapons (Whyte & Mazanec, 2019). So, if they occurred, the fact that they were not in traditional news media was a good sign for either the GC's approach or news media's discretion with respect for national security. Public attribution of cyber attacks from foreign threat actors and GC defensive cyber activity were dominant across both periods.

Foreign Interference – Cyber Security and Geopolitics

Geopolitics matter immensely in cyber security to understand the threat landscape, inform GC cyber operations, and for Canada's alliances. CSIS has identified over 30 countries taking steps to include cyber warfare capacities within military organizations and planning and some argue that cyber warfare as a "brute force" weapon will likely increase. Countries like China are increasingly developing warfighting strategies that are information-based (Whyte & Mazanec, 2019).

During the periods of analysis public attributions were made against both China and Russia for specific attacks, and they remain threat actors. Chinese cyber attacks were nothing new for Canada and it was no surprise that intellectual property theft and cyber espionage were ongoing themes. In 2011 an attack targeted at Defence Research and Development Canada was detected, forcing the Finance Department and Treasury Board off the internet and an investigation into how much sensitive information had been taken. Later in 2014 the Communications Security Establishment detected a cyberattack targeting the National Research Council (Van Wie Davis, 2021). Information and data sovereignty are essential to Canada's competitive advantage and national security so safeguarding against these attacks is critical. Sometimes public shaming is used as a form of deterrence, but making public attributions is a challenge because there is the potential for retaliation due to the diplomatic reputational impact. When the GC makes public attributions, it is a considered decision. Attributions made by the GC were all in support of, or in collaboration with, allies implying dissemination or potentially asymmetrical models because it is messaging the GC wants allies to hear – that Canada stands with them. Asymmetrical could not be fully evaluated in this research model.

This research spanned a specific period in Canadian history where Huawei 5G was high visibility in cyber security, diplomatic, geopolitical, national security, and defence contexts. The cyber security side of the Huawei 5G story was central to 38.5% of the articles reviewed in 2018 and 13.4% in 2021. It was already known that state controlled Chinese Telcom had ten internet points of presence and had been involved in the "hijacking, diverting, and then copying of rich traffic going into or crossing the Unites States and Canada" (Van Wie Davis, 2021). Allies were urging action, but there were also Canadian lives on the line with the two Michaels amongst a range of other geopolitical considerations. Now that Canada has made the decision to ban Huawei from 5G networks as well as terminate or remove existing Huawei 4G equipment with no new purchases of Huawei 4G or 5G equipment as of September 2022 (Zimonjic, 2021) GC cyber security themes in news media will shift, but likely not too far. What this meant for the model of government-media relations during both time periods was that there were a range of considerations in the decision-making process, so messaging had to be targeted. The audience included the Canadian public, allies, and the Chinese government. The implications of a misstep would have put added pressure on the already strained relationship. As evidenced throughout, the model was predominantly information dissemination and this story particularly had targeted repeated messages, which could imply asymmetrical which could not be assessed herein.

Interestingly, election interference and cyber security was a greater referenced topic in news media in 2018 with the election coming in 2019 than it was in 2021 for the election that was called and fell within the period of analysis. There were several factors that could have been involved. In 2018 there were reports of Russian election meddling

in the United States heightening concerns of preserving Western democracies, so it was on the media agenda in general. In 2021 there may also have been less cause for alarm since the previous election had no evidence of interference and lessons learned were integrated. Other factors could have included the quick election period or the extent of other high visibility things on the news media's radar like COVID-19 and attacks on critical infrastructure including healthcare with finite journalistic resources in traditional news.

The fact that politicized issues like China got the most coverage, meant that of course other things do not get coverage, including Get Cyber Safe tools to support Canadians and businesses. Having the public engaged could have increased Canada's overall cyber resilience. Only once was a Get Cyber Safe tool picked up and it was around being cyber safe in holiday gift purchasing. There were many other tools that could have been used in the public interest. General awareness of cyber hygiene, best practices, and GC programming or points of contact to report malicious activity could reduce risk and support the GC in addressing cyber incidents. That these were not picked up by media is indicative of the government-media relations model. The GC's relationships with news media can influence the extent to which and how GC messages, strategies, policies, and programs get represented. These kinds of good news stories were not picked up indicating that if the GC was trying to disseminate them, the media did not have an appetite or there was not public engagement in cyber security.

Conclusions and Recommendations

The GC's ability to communicate can impact the uptake of programming and overall cyber resilience so government-media relations are important. Cyberweapons are being embraced by governments and militaries for some obvious reasons. They may offer

anonymity, be perceived as lower collateral damage than other attacks, are faster than missiles, and zero-day vulnerabilities can be tweaked as patches are made pulling from reserves of alternate exploits (Zetter, 2014). This can lead to advanced persistent threats, which pose national security threats. Telecommunications networks were of high concern for the public. Security of those networks was a prime concern across both periods, not just for Canada but allies as well. The other major themes also involved GC defensive cyber operations, foreign interference, or privacy concerns. The model of government-media relations for the GC on cyber security was predominantly evidenced to be dissemination of information but had indications of elements from asymmetric communications that could not be confirmed within this research model. GC messaging was to engender public and allied confidence and targeted.

Throughout the content analysis there was no evident political spin or smut story style of reporting demonstrating professionalism. This takes the publicity model of government-media relations off the table as there were no promotional stories. Since the majority of articles across both periods leveraged GC speaking points and content it is indicative of a dissemination of information model and symbiotic relationship between the GC and news media.

Most reporting was just factual, but when there was slant it was more often ambiguous or negative, which indicated that the press was still performing an important democratic challenge function. This could be indicative of a two-way model of government-media relations, which unfortunately could not be confirmed within this research model due to lack of visibility into internal documentation or planning. It could be intuited that with the subject of interest being GC activities and programming in cyber

security that the GC was at an information advantage in communications, though the intent and approach to those communications could not be gleaned from this research.

Geopolitics was important to what got picked up in Canadian news media. This might have been because Canada relies heavily on alliances and much of the messaging was intended to demonstrate strength for allies as well as engendering public trust. Canada has been under attack from foreign threat actors and must continue to increase cyber resilience, capabilities, and engage collaboratively with allies to face this shadow warfare. It was not surprising that this was central in many storylines. There were some missed opportunities in these periods.

Cyber crime was an increasing concern for Canadians and yet there was almost no representation of Get Cyber Safe containing lots of public-facing content intended to support Canadian public and businesses. It could be beneficial for the GC to work with news media to publicize resources like these, if possible, to mitigate some of the concerns raised in negatively skewed articles on GC's approach to cyber crime. Perhaps the public is simply unaware of or has not had the interest to dig into these tools to see what might serve their needs. Communications approaches with regards to cyber security should consider the scope of public interest and full range of audiences. It is evidenced from the increase in scrutiny over the second period that there are gaps to be addressed concerning the public and news media related to cyber crime and privacy.

Works Cited

(DND), D. o. (2017). *Strong Secure Engaged: Canada's Defence Policy.* Copyright Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2017.

Agence France-Presse. (2021, September 25). Meng Wanzhou and the two Michaels: a timeline. *The Guardian*.

Apparlraju, Y. (2021, December 11). Transforming cybersecurity from threat mitigator to innovation enabler. *Toronto Star*.

Arthur, B. (2018, October 4). Bruce Arthur: Russian hackers have become the spies who love. *Toronto Star*.

Arthur, B. (2018, October 5). Faster, stronger and ... spy-er? RUSSIA. *Toronto Star*.

Associated Press. (2018, November 12). Cinquante pays signent un pacte. *Le Droit*.

Bailey, I. (2021, December 2). Politics Briefing: Governor-General's office investigating internal network breach. *The Globe and Mail*.

Bailey, I. (2021, December 13). Thousands of websites go offline over cybersecurity threat. *The Globe and Mail*.

Bailey, I. (2021, December 12). Thousands of websites go offline over cybersecurity threat. *The Globe and Mail*.

Berthiame, L. (2021, July 17). Cyber agency warns foreign ‘actors' pose threat to Canada's next election. *The Globe and Mail*.

Berthiame, L. (2021, July 17). Cyberagency warns of election targeting. *Toronto Star*.

Berthiaume, L. (2021, July 20). Front commun de l'Occident pour dénoncer la Chine. *La Presse*.

Berthiaume, L. (2021, July 19). Le Canada et des alliés tiennent la Chine responsable d'une cyberattaque massive. *Le Droit*.

Berthiaume, L. (2021, July 19). Le Canada et des alliés tiennent la Chine responsable d'une cyberattaque massive. *Le Droit*.

Black, C. (2018, December 15). Canada remains a nation of laws. The U.S., meanwhile. *National Post*.

Blackley, S. (2018, December 21). Morning Update: Bell, Telus warn of 5G delays, higher costs if Huawei banned; U.S. Defence Secretary Mattis resigns; Also: Canada joins U.S., Britain in calling out China for state-sponsored hacking campaign; B.C. voters reject proportional representation. *The Globe and Mail*.

Blanchfield, M. (2018, December 7). Business facing risk of retaliation; ANALYSTS. *National Post*.

Blanchfield, M. (2018, October 5). Canada blames Russia for hacks; NATO countries claim cyberattack targeted anti-doping agency. *Toronto Star*.

Boutilier, A. (2017, January 27). *Canada's allies racing ahead on boosting cybersecurity, PM told*. Retrieved from Toronto Star: https://www.thestar.com/news/canada/2017/01/27/canadas-allies-racing-ahead-on-boosting-cyber-security-pm-told.html

Boutilier, A. (2018, October 8). Bracing for election meddling; Provinces get primer from national spy group. *Toronto Star*.

Boutilier, A. (2018, November 23). Election meddling a threat, Ottawa says; 'Virtually impossible' to prevent foreign interests from spreading misinformation, minister warns. *Toronto Star*.

Boutilier, A. (2018, October 6). Feds brief provinces on election interference threat. *Toronto Star*.

Boutilier, A. (2018, November 22). 'Virtually impossible' to prevent foreign meddling in 2019 election, Karina Gould says. *Toronto Star*.

Boutilier, A. (2018, November 22). 'Virtually impossible' to prevent foreign meddling in 2019 election, Karina Gould says. *Toronto Star*.

Boutilier, A. (2021, July 19). Canada joins allies in linking China to Microsoft email hack. *Toronto Star*.

Boutilier, A. (2021, July 20). Canada joins allies in linking China to Microsofthack. *Toronto Star*.

Brearton, S., & Calleja, D. (2018, September 28). Tech Support. *The Globe and Mail*.

Bronskill, J. (2018, December 21). Canada among hacking targets; Two Chinese citizens charged with waging a campaign to steal data. *Toronto Star*.

Bronskill, J. (2021, November 15). Canada has no choice but to bar Huawei from 5G networks, security experts say. *The Globe and Mail*.

Bronskill, J. (2021, November 15). Canada has no choice but to bar Huawei from 5G networks, security experts say. *The Globe and Mail*.

Bronskill, J. (2021, November 14). Des experts en sécurité disent que le Canada doit exclure Huawei de. *Le Droit*.

Bronskill, J. (2021, November 14). Des experts en sécurité disent que le Canada doit exclure Huawei de. *Le Droit*.

Bronskill, J. (2021, November 15). Des experts en sécurité disent que le Canada doit exclure Huawei de. *Le Droit*.

Burney, D. (2018, September 26). How prepared is Canada for cyberattacks ? In an ever-shifting America-first world, we shouldn't rely on our neighbour to continue to share their technology with alacrity, as economic competitiveness intensifies. *The Globe and Mail*.

Calleja, D., & Brearton, S. (2018, September 28). How to hack-proof your employees; It's just a matter of time before your company suffers a data breach (if it hasn't already). Here's how to lock down your network—and your employees. *The Globe and Mail*.

Campion, B. (2018, December 20). Canadian air force aircraft harassed by Chinese during patrols off North Korea. *Toronto Star*.

Campion, B. (2018, December 4). Growing threat of espionage threatens Canada's economic interests, spy agency head warns. *Toronto Star*.

Campion-Smith, B. (2018, December 5). Spies after corporate intel, CSIS warns; Agency head says current state-sponsored interference a real threat. *Toronto Star*.

Canada, G. o. (2022, May 5). *Get Cyber Safe*. Retrieved from Canada.ca: https://www.getcybersafe.gc.ca/en

Canadian Association of Journalists. (2011, June). *Ethics Guidelines*. Retrieved from Canadian Association of Journalists: https://caj.ca/ethics-guidelines

Canadian Centre for Cyber Security (CCCS). (2018, November 2). *CSE's security review program for 3G/4G/LTE in Canadian telecommunications networks*. Retrieved from News: https://cyber.gc.ca/en/news/cses-security-review-program-3g4glte-canadian-telecommunications-networks

Canadian Centre for Cyber Security (CCCS). (2020, November 30). *Cyber threat bulletin: Modern ransomware and its evolution*. Retrieved from Publications: https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-modern-ransomware-and-its-evolution

Canadian Centre for Cyber Security (CCCS). (2021, December 22). *Active exploitation of Apache Log4j vulnerability - Update 6*. Retrieved from Alerts: https://cyber.gc.ca/en/alerts/active-exploitation-apache-log4j-vulnerability

Canadian Centre for Cyber Security (CCCS). (2021, May 13). *Baseline cyber security controls for small and medium organizations*. Retrieved from Publications: https://cyber.gc.ca/en/guidance/baseline-cyber-security-controls-small-and-medium-organizations

Canadian Centre for Cyber Security (CCCS). (2021, September 13). *Information and Guidance*. Retrieved from Home: https://cyber.gc.ca/en/information-guidance

Canadian Centre for Cyber Security (CCCS). (2022, May 31). *Follina vulnerability impacting Microsoft products*. Retrieved from Alerts & Advisories.

Canadian Space Agency (CSA). (2020, October 23). *Quantum Encryption and Science Satellite (QEYSSat)*. Retrieved from Satellites: https://www.asc-csa.gc.ca/eng/satellites/qeyssat.asp

Carmichael, A., & Ahmad, I. (2018, December 18). Cybersecurity breaches will soon reverberate all the way up to the board level; Canada's new mandatory data-breach notification rule means boards can no longer afford to be deferential toward cyberattacks. *The Globe and Mail*.

Carmichael, A., & Ahmad, I. (2018, December 18). Cybersecurity issues will soon reverberate all the way up to the board level. *The Globe and Mail*.

Carrick, R. (2021, December 10). This is how much allowance kids are getting these days. *The Globe and Mail*.

Carrick, R. (2021, December 9). This is how much allowance kids are getting these days. *The Globe and Mail*.

Carvin, S., & Juneau, T. (2021, September 9). Canada's exclusion from 'Three Eyes' only affirms the reality. *The Globe and Mail*.

Castaldo, J. (2018, October 28). Many companies not ready for new data-breach response rules, experts say. *The Globe and Mail*.

Castaldo, J. (2021, August 14). Locked out: The growing risk of ransomware hackers has governments, insurers and cybersecurity experts scrambling. *The Globe and Mail*.

Castaldo, J. (2021, August 14). Locked out: The growing risk of ransomware hackers has governments, insurers and cybersecurity experts scrambling. *The Globe and Mail*.

Castaldo, J. (2021, August 14). Under Attack. *The Globe and Mail*.

Castaldo, J. (2021, August 14). Under Attack. *The Globe and Mail*.

Castelvecchi, D. (2022, February 8). *https://www.nature.com/articles/d41586-022-00339-5*. Retrieved from nature: https://www.nature.com/articles/d41586-022-00339-5

Champagne, S. (2021, October 4). La physique quantique à la rescousse. *La Presse*.

Chase, S. (2018, December 21). Canada joins allies in condemning China's hacking campaign. *The Globe and Mail*.

Chase, S. (2018, October 5). Canada joins censure of Russian hacking. *The Globe and Mail*.

Chase, S. (2018, December 20). Canada joins U.S., U.K. in calling out China for state-sponsored hacking campaign; The move comes as Canada is weighing whether to allow Huawei Technologies to supply gear for next-generation 5G mobile networks. *The Globe and Mail*.

Chase, S. (2018, October 4). Canada, Western allies rebuke Russia over alleged global. *The Globe and Mail*.

Chase, S. (2021, November 21). Former Australian PM Malcolm Turnbull says Huawei 5G would leave Canada's networks vulnerable to China. *The Globe and Mail*.

Chase, S. (2021, November 20). Former Australian PM Malcolm Turnbull says Huawei 5G would leave Canada's networks vulnerable to China. *The Globe and Mail*.

Chase, S. (2021, November 21). Former Australian PM Malcolm Turnbull says Huawei 5G would leave Canada's networks vulnerable to China. *The Globe and Mail*.

Chase, S. (2021, November 20). Former Australian PM Malcolm Turnbull says Huawei 5G would leave Canada's networks vulnerable to China. *The Globe and Mail*.

Chase, S., & Fife, R. (2018, October 12). U.S. senators urge Trudeau to block Huawei from 5G. *The Globe and Mail*.

Chase, S., & Fife, R. (2018, October 12). U.S. senators urge Trudeau to block Huawei from 5G. *The Globe and Mail*.

Chase, S., & Fife, R. (2018, October 12). U.S. senators urge Trudeau to block Huawei from 5G. *The Globe and Mail*.

Chase, S., & Fife, R. (2018, October 12). U.S. senators urge Trudeau to block Huawei from 5G; In letter to PM, two senior committee members warn inadequate safety

measures put Canadian national security and ‘Five Eyes’ joint intelligence. *The Globe and Mail*.

Chase, S., & Fife, R. (2018, October 12). U.S. senators urge Trudeau to block Huawei from 5G; In letter to PM, two senior committee members warn inadequate safety measures put Canadian national security and ‘Five Eyes’ joint intelligence. *The Globe and Mail*.

Chase, S., & Fife, R. (2018, October 12). U.S. senators urge Trudeau to block Huawei from 5G; In letter to PM, two senior committee members warn inadequate safety measures put Canadian national security and ‘Five Eyes’ joint intelligence. *The Globe and Mail*.

Chase, S., Fife, R., & McKenna, B. (2018, October 16). Trudeau defends Huawei policy amid national security concerns. *The Globe and Mail*.

Chase, S., Zilio, M., & VanderKlippe. (2018, December 20). Detention of third Canadian doesn't appear to be tied to Huawei, PM says. *The Globe and Mail*.

Chase, S., Zilio, M., & VanderKlippe. (2018, December 20). Detention of third Canadian doesn't appear to be tied to Huawei, PM says. *The Globe and Mail*.

Chase, S., Zilio, M., & VanderKlippe, N. (2018, December 19). Teacher Sarah McIver third Canadian detained in China; Trudeau says doesn’t appear to be retaliation for Huawei arrest; Trudeau said details obtained so far suggest this third case is more of a routine matter and different from the Dec. 10 detentions of f. *The Globe and Mail*.

Chase, S., Zillo, M., & VanderKlippe, N. (2018, December 19). Teacher Sarah McIver third Canadian detained in China; Trudeau says doesn’t appear to be retaliation

for Huawei arrest; Trudeau said details obtained so far suggest this third case is more of a routine matter and different from the Dec. 10 detentions of f. *The Globe and Mail*.

Chiu, J., & Grauer, P. (2018, December 6). Federal government under fire for Canada's Huawei ties. *Toronto Star*.

Chiu, J., & Grauer, P. (2018, December 6). Federal government under fire for Canada's Huawei ties following arrest in Vancouver. *Toronto Star*.

Chiu, J., & Grauer, P. (2018, December 6). Federal government under fire for Canada's Huawei ties following arrest in Vancouver. *Toronto Star*.

Chiu, J., & Grauer, P. (2018, December 6). Huawei arrest fuels anxiety over the security of Canada's 5G dealings. *Toronto Star*.

Codère, J.-F. (2018, October 5). La Chine prise la main dans le sac. *La Presse*.

Cook, L. (2018, October 4). Plusieurs pays, dont le Canada, accusent la Russie de cybercriminalité. *La Presse*.

Curry, B. (2018, November 2). Privacy watchdog probes Statscan move to collect personal banking data. *The Globe and Mail*.

Curry, B. (2018, November 2). Statscan must justify request for personal banking data, former chief says. *The Globe and Mail*.

Da Silva, M., & Augustin, M. (2022, July 8). *The Rogers outage is disrupting services across Canada. A list of what is affected*. Retrieved from The Globe and Mail: https://www.theglobeandmail.com/business/article-rogers-interac-outage-services/

Dawson, P., & Ouimette, M.-É. (2021, September 7). Tech and geopolitics are on a collision course. Is Canada ready? *The Globe and Mail*.

Dobby, C. (2018, December 21). Bell, Telus warn of 5G delays, higher costs if Ottawa joins peers. *The Globe and Mail*.

Dobby, C. (2018, December 21). Bell, Telus warn of 5G delays, higher costs if Ottawa joins peers in banning Huawei; They argue that security concerns related to Huawei can be addressed by testing its equipment and restricting its gear to non-sensitive parts of their networks. *The Globe and Mail*.

Donovan, K. (2018, November 27). Have you been hacked or phished? The Mounties want to know. *Toronto Star*.

Donovan, K. (2018, November 29). RCMP dives into phishing probe; In effort to crack down on cybercrime, asking victims to report cases. *Toronto Star*.

Duquette, P. (2021, November 30). Ces terrifiants pirates du Web. *Le Droit*.

Duquette, P. (2021, December 1). Ces terrifiants pirates du Web. *Le Droit*.

Elections Canada. (2021, September). *September 20, 2021 General Election National Results*. Retrieved from Elections Canada: https://www.elections.ca/enr/help/national_e.htm

Emmot, R. (2021, October 22). NATO plan aims to deter Russia aggression; Puts focus on Baltics, Black Sea regions. *National Post*.

Emmott, R. (2021, October 22). NATO plan aims to deter Russia aggression; Puts focus on Baltics, Black Sea regions. *Ottawa Citizen*.

Fife, R. (2021, July 20). Canada joins allies in denouncing China for global Microsoft. *The Globe and Mail*.

Fife, R. (2021, July 19). Canada joins allies in denouncing China for global Microsoft. *The Globe and Mail*.

Fife, R. (2021, July 20). Canada, allies condemn China for cyberattack on Microsoft. *The Globe and Mail*.

Fife, R. (2021, November 15). Federal cabinet will rule soon on whether to ban Huawei from 5G. *The Globe and Mail*.

Fife, R. (2021, September 28). Federal cabinet will rule soon on whether to ban Huawei from 5G. *The Globe and Mail*.

Fife, R. (2021, December 9). New U.S. ambassador to Canada says China is greatest threat to democracy, urges Ottawa to align with U.S. to challenge Beijing. *The Globe and Mail*.

Fife, R. (2021, December 10). U.S. envoy warns Canadians about China. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, December 7). China demands release of Huawei executive. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 31). China Telecom diverted internet traffic in U.S. and Canada, report finds; Cybersecurity researchers say state-owned firm has shunted data through legal access points in North America in an effort to steal intellectual property. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 31). China Telecom diverted internet traffic in U.S. and Canada, report finds; Cybersecurity researchers say state-owned firm has shunted data through legal access points in North America in an effort to steal intellectual property. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 31). China Telecom diverted online traffic, report says. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, December 17). Five Eyes spy chiefs warned Trudeau twice about Huawei national-security risk; Sources said the spy chiefs stressed that their countries cannot become dependent upon Huawei's 5G technology. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, December 17). Five Eyes spy chiefs warned Trudeau twice about Huawei national-security risk; Sources said the spy chiefs stressed that their countries cannot become dependent upon Huawei's 5G technology. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, December 17). Five Eyes spy chiefs warned Trudeau twice on Huawei risk. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, December 17). Five Eyes spy chiefs warned Trudeau twice on Huawei risk. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, December 19). Huawei chairman challenges security risk concerns, demands proof that tech giant is a pawn of Beijing. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, December 19). Huawei chairman challenges security risk concerns, demands proof that tech giant is a pawn of Beijing; Huawei chairman warned that banning Huawei from supplying next-generation 5G mobile technology to Western countries would raise costs to consumers and s. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 26). Huawei executives lobbied MPs to resist U.S. 5G boycott effort; Representatives of the Chinese telecom began an influence

campaign in late August after Australia joined the United States as the second Five Eyes intelligence ally to block the company from . *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 26). Huawei executives lobbied MPs to resist U.S. 5G boycott effort; Representatives of the Chinese telecom began an influence campaign in late August after Australia joined the United States as the second Five Eyes intelligence ally to block the company from . *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 26). Huawei lobbies MPs to thwart U.S. 5G boycott effort. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 26). Huawei lobbies MPs to thwart U.S. 5G boycott effort. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, November 29). New Zealand bans Huawei gear, following U.S. and Australia. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, November 29). New Zealand bans Huawei gear, following U.S. and Australia. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, November 29). New Zealand becomes third Five Eyes member to ban Huawei from 5G network; New Zealand is barring China’s Huawei on national-security grounds from supplying equipment for next-generation mobile networks. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, November 29). New Zealand becomes third Five Eyes member to ban Huawei from 5G network; New Zealand is barring China’s Huawei on national-security grounds from supplying equipment for next-generation mobile networks. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, September 23). No need to ban Huawei in light of Canada's robust cybersecurity safeguards, top official says; Head of cybersecurity dismisses calls to join U.S. and Australia in blocking Chinese firm. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, September 24). No need to ban Huawei, Ottawa says. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, September 19). Ottawa launches probe of cyber security. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, September 19). Ottawa launches probe of cyber security; Australia and U.S. have already imposed ban on China's Huawei from participating in new wireless cellular networks. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, November 2). Ottawa not ruling out blocking Huawei from 5G supply contracts; Review under way to determine whether Canada should join the U.S. and Australia in banning Chinese telecommunications giant, Goodale says. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, November 2). Ottawa not ruling out blocking Huawei from 5G supply contracts; Review under way to determine whether Canada should join the U.S. and Australia in banning Chinese telecommunications giant, Goodale says. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, September 7). Ottawa probes Huawei devices for security threats. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, September 7). Ottawa probes Huawei equipment for security threats; Facing U.S. pressure to ban Chinese firm's equipment from 5G networks,

federal government acknowledges for first time that it has been conducting tests since 2013. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, November 2). Ottawa reconsiders blocking Huawei from 5G work. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, November 2). Ottawa reconsiders blocking Huawei from 5G work. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, July 30). Ottawa sees Chinese-owned Huawei as major security threat, senior officials say; Trudeau government and allies alarmed by high-tech giant's growing dominance in 5G telecommunications technology. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, July 30). Ottawa's worries grow over global ambitions of Huawei. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, December 7). Trudeau says he knew about the arrest of a top Huawei executive; Meng Wanzhou was picked up by Canadian law enforcement officials in transit at Vancouver airport Dec. 1. at the request of U.S. authorities. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 10). U.S. intelligence officials question Canada's ability to test China's Huawei for security breaches; Senior officials reportedly laugh at declaration that Canada possesses sufficient safeguards to address risks posed by telecom giant. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 1). U.S. intelligence officials question Canada's ability to test China's Huawei for security breaches; Senior officials reportedly

laugh at declaration that Canada possesses sufficient safeguards to address risks posed by telecom giant. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 1). U.S. intelligence officials question Canada's ability to test China's Huawei for security breaches; Senior officials reportedly laugh at declaration that Canada possesses sufficient safeguards to address risks posed by telecom giant. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 1). U.S. security officials question Canada's ability to test Huawei risks. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 1). U.S. security officials question Canada's ability to test Huawei risks. *The Globe and Mail*.

Fife, R., & Chase, S. (2018, October 1). U.S. security officials question Canada's ability to test Huawei risks. *The Globe and Mail*.

Fife, R., & Curry, B. (2021, December 17). PM presses for Canada to become a critical mineral powerhouse. *The Globe and Mail*.

Fife, R., & Curry, B. (2021, December 16). PM presses for Canada to become a critical mineral powerhouse. *The Globe and Mail*.

Fife, R., Chase, S., & Bailey, I. (2018, August 24). Australia joins U.S. in ban of Huawei from 5G network. *The Globe and Mail*.

Fife, R., Chase, S., & Bailey, I. (2018, August 28). Trudeau won't say if Canada will follow Australia, U.S. in blocking Huawei from big projects; The world's largest maker of telecommunications-network equipment and the No. 3 smartphone supplier, has already been virtually shut out of the U.S. market. *The Globe and Mail*.

Fife, R., Chase, S., & Freeze, C. (2018, December 5). CSIS chief warns of state-sponsored espionage threat to 5G networks. *The Globe and Mail*.

Fife, R., Chase, S., & Freeze, C. (2018, December 4). CSIS director warns of state-sponsored espionage threat to 5G networks; David Vigneault told a business audience that hostile states are targeting large companies and universities to obtain new technologies, but refrained from naming any particular countr. *The Globe and Mail*.

Freeze, C. (2018, October 3). Cyber czar says Canada has ‘layers' to protect against potential Huawei threat. *The Globe and Mail*.

Freeze, C. (2018, October 2). Ottawa’s top cybersecurity official: Canada has ‘layers’ to protect against Huawei threat; Washington has been putting pressure on Canada, Britain and New Zealand to join the United States and Australia in banning Huawei from supplying equipment for the C. *The Globe and Mail*.

Freeze, C. (2021, November 3). Newfoundland cyberattack an 'alarm bell' for Canada. *The Globe and Mail*.

Freeze, C. (2021, November 1). Newfoundland cyberattack an 'alarm bell' for Canada. *The Globe and Mail*.

Friesen, J. (2021, July 26). CSIS warns Canadian universities to be on alert for international espionage. *The Globe and Mail*.

Friesen, J. (2021, July 26). CSIS warns Canadian universities to be on alert for international espionage. *The Globe and Mail*.

Gagnon, C. A. (2021, September 9). Trafic d'armes à feu: le fédéral doit. *Le Droit*.

Gagnon, C.-A. (2021, September 8). Lutte au trafic des armes à feu: le fédéral doit faire preuve d'un. *Le Droit*.

Gagnon, C.-A. (2021, September 8). Lutte au trafic des armes à feu: le fédéral doit faire preuve d'un «leadership fort», selon les directeurs de police du Québec. *Le Droit*.

Gagnon, C.-A. (2021, September 9). Trafic d'armes à feu: le fédéral doit. *Le Droit*.

Get Cyber Safe. (2021, November 8). *Celebrating 10 years of Get Cyber Safe*. Retrieved from Get Cyber Safe - Resources: https://www.getcybersafe.gc.ca/en/resources/celebrating-10-years-get-cyber-safe

Glavin, T. (2021, September 16). A giant panda in the room; Liberals can't bear to talk about China. *National Post*.

Glavin, T. (2021, September 16). A giant panda in the room; Liberals can't bear to talk about China. *National Post*.

Government of Canada. (2018, September 25). *Government of Canada Announces New National Cyber Security Strategy and the Creation of the Canadian Centre for Cyber Security*. Retrieved from Canadian Centre for Cyber Security - Publications: https://cyber.gc.ca/en/guidance/government-canada-announces-new-national-cyber-security-strategy-and-creation-canadian

Government of Canada. (2021, September 1). *Section 2(b) – Freedom of expression*. Retrieved from Charterpedia: https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art2b.html

Grammond, S. (2021, December 20). Un ministre contre les pirates. *La Presse*.

Grammond, S. (2021, December 20). Un ministre contre les pirates. *La Presse*.

Green, M. (2018, November 8). Canada should oust Chinese telecom Huawei, say security experts. *Toronto Star*.

Gurney, M. (2021, November 5). Cyberattack should be a wake-up call. *National Post*.

Hannay, C. (2018, December 21). Politics Briefing: Trudeau's carbon-tax fight is getting more complicated; Also: Canada condemns Chinese hacking. *The Globe and Mail*.

Hannay, C., & James, K. (2018, October 3). Politics Briefing: LNG project good for business, but may threaten environment; Also: Trudeau says Canada-China trade won't be stopped by USMCA clause. *The Globe and Mail*.

Hannay, C., & Keller, C. (2018, October 1). Politics Briefing: The new trade deal is here; Also: Quebec votes today. *The Globe and Mail*.

Hannay, C., & Keller, J. (2018, September 24). Politics Briefing: Government workers told to stay home after Ottawa tornado; Also: Trudeau in New York. *The Globe and Mail*.

Hannay, C., & Keller, J. (2019, September 19). Politics Briefing: Canada not making concessions, Republican charges; Also: Ottawa launches cyber security analysis. *The Globe and Mail*.

Held, M. (2018, March 5). *Budget 2018 Takes Cyber Crime Seriously, And So Should Canadians*. Retrieved from Huffpost.ca: https://www.huffingtonpost.ca/matthew-held/cyber-crime-canadian-small-businesses_a_23374814/

Holland, B. (2021, December 15). The underfunding of Canadian health care makes it vulnerable to cyberthreats. *The Globe and Mail*.

House, K. (2018, September 26). It's About Competition. *The Globe and Mail*.

House, K. (2018, September 26). It's About Competition. *The Globe and Mail*.

Hunnicutt, T., Bose, N., Brunnstrom, D., & Packham, C. (2021, September 17). China, France denounce new nuclear sub pact; Australia to get technology from U.S., U.K. *National Post*.

Israel, T., & Tribe, L. (2018, October 15). Did NAFTA 2.0 sign away Canada's digital future?; Deal demonstrates lack of foresight, Tamir Israel and Laura Tribe write. *The Ottawa Citizen*.

Jackson, E. (2018, December 7). Huawei arrest puts telecom ties in glare; Canada pressed to re-evaluate relationship. *National Post*.

Jackson, E. (2018, December 7). Huawei arrest puts telecom ties in glare; Canada pressed to re-evaluate relationship. *National Post*.

Jackson, E. (2018, December 7). Huawei exec's arrest puts focus on Chinese company's ties in Canada; Universities with research partnerships say it's business as usual, telecoms mum. *The Ottawa Citizen*.

Jackson, E. (2018, December 7). Huawei exec's arrest puts focus on Chinese company's ties in Canada; Universities with research partnerships say it's business as usual, telecoms mum. *The Ottawa Citizen*.

Jackson, E. (2018, December 20). Huawei pledges cyber security; 5G Networks; 'Whatever'Canada requires, China giant says. *National Post*.

Jackson, E. (2018, October 3). Website-blocking plan to fight online piracy rejected by CRTC. *The Ottawa Citizen*.

Karadeglija, A. (2021, November 13). Banning Huawei a 'no-brainer' , say analysts; Would be bold. *National Post*.

Karadeglija, A. (2021, November 13). Banning Huawei a 'no-brainer' , say analysts; Would be bold stroke but strong message to china and our allies. *National Post*.

Krol, A. (2018, November 8). StatCan et votre compte de banque. *La Presse*.

La Press+. (2018, November 13). Cinquante pays s'unissent contre la cybercriminalité. *La Presse*.

La Presse canadienne. (2018, November 12). Cinquante pays signent un pacte. *Le Droit*.

La Presse Canadienne. (2018, December 21). Le Canada aurait été lui aussi la cible de pirates informatiques chinois. *Le Droit*.

La Presse canadienne. (2018, October 15). Les entreprises ont dépensé 14. *Le Droit*.

Lapierre, M. (2021, December 20). Dark web, new wave of criminals tied to rise in area cyber attacks; OPP cybercrime unit tracks hackers, data breaches, ransomware incidents. *Ottawa Citizen*.

Latouche, M. (2018, November 2). StatCan gets too snoopy. *National Post*.

Ligeti, A. (2018, October 31). Morning Update: A last-minute deal to save Calgary's Olympic bid; Chinese firm diverted web traffic; Also: Canadian hospitals are reporting a spike in a rare syndrome resembling polio. *The Globe and Mail*.

Ligeti, A. (2018, November 28). Morning Update: Charges stayed in major B.C. money-laundering case; another Five Eyes ally bars Huawei from 5G;. *The Globe and Mail*.

Ligeti, A. (2018, September 19). Morning Update: Opioids killing 11 Canadians daily; Facebook shuts down accounts linked to Vancouver election; Also: Ottawa has launched a probe of cyber security. *The Globe and Mail*.

MacCharles, T. (2018, December 7). PM denies role in arrest of Chinese exec; Trudeau says he had 'a few days' notice' of Canada's move to comply with FBI request. *Toronto Star*.

MacCharles, T. (2018, December 6). Trudeau says he had nothing to do with the arrest of Chinese executive in Vancouver. *Toronto Star*.

MacDonald, M., & Doucette, K. (2018, November 18). Élections fédérales: Ottawa. *Le Droit*.

MacDonald, M., & Doucette, K. (2018, November 18). Next Canadian federal election will be target for Russian meddling, says Harjit Sajjan. *Toronto Star*.

MacDonald, M., & Doucette, K. (2018, November 19). Voters warned of meddling in 2019 election; Russian efforts cyber-security plan touted by defence minister. *The Ottawa Citizen*.

MacDonald, M., & Doucette, K. (2018, November 19). Voters warned of meddling in 2019 election; Russian efforts cyber-security plan touted by defence minister. *National Post*.

MacDonald, M., & Doucette, K. (2018, November 19). Voters warned of meddling in 2019 election; Russian efforts cyber-security plan touted by defence minister. *National Post*.

MacDonald, M., & Doucette, K. (2018, November 19). Voters warned of meddling in 2019 election; Russian efforts cyber-security plan touted by defence minister. *The Ottawa Citizen*.

MacKinnon, M. (2021, October 22). Russia's break with NATO heightens fears of military escalation as two sides trade blame. *The Globe and Mail*.

MacKinnon, M. (2021, October 21). Russia's break with NATO heightens fears of military escalation as two sides trade blame. *The Globe and Mail*.

Mateo, A. G., & Bhatia, A. (2021, August 7). Facial-recognition surveillance threatens our rights. *Toronto Star*.

Mateo, A. G., & Bhatia, A. (2021, August 7). Facial-recognition surveillance threatens our rights. *Toronto Star*.

Mateo, A. G., & Bhatia, A. (2021, July 29). Reports find that federal government surveillance was again used at Pearson airport, this time through facial recognition. This threatens our human rights. *Toronto Star*.

Mateo, A. G., & Bhatia, A. (2021, July 29). Reports find that federal government surveillance was again used at Pearson airport, this time through facial recognition. This threatens our human rights. *Toronto Star*.

McCall, J. (2018, December 27). Unprincipled Giants. *The Globe and Mail*.

McKenna, B. (2018, December 24). Now is not the time for Canadian businesses to retreat from China. *The Globe and Mail*.

McKenna, B. (2018, December 23). Now is not the time for Canadian businesses to retreat from China; Canada must look past current concerns to protect future growth in mutually beneficial dealings between the two countries. *The Globe and Mail*.

Mcleod, J. (2018, October 5). Concerns Over Data Localization Ban In Usmca Could Be Overblown; New trade deal may have provision that allows for carveout, James McLeod writes. *The Ottawa Citizen*.

Mcleod, J. (2018, October 5). Data localization fears may be inflated; Usmca. *National Post*.

Mcleod, J. (2018, October 31). New data breach rules not strong enough, critics argue. *National Post*.

Mcleod, J. (2018, October 31). New rules for data breach don't go far enough, critics warn. *The Ottawa Citizen*.

Miró, R. (2021, October 4). Les gouvernements en font-ils assez ? *La Presse*.

Morrow, A. (2021, September 16). Canada left out as U.S., U.K., Australia strike deal to counter China. *The Globe and Mail*.

Morrow, A. (2021, September 16). Canada left out as U.S., U.K., Australia strike deal to counter China. *The Globe and Mail*.

Morrow, A. (2021, September 15). Canada left out as U.S., U.K., Australia strike deal to counter China. *The Globe and Mail*.

Nardi, C. (2021, December 7). 235 known ransomware attacks so far in 2021; Canadian centre says most activity unreported. *National Post*.

Nardi, C. (2021, December 7). 235 known ransomware attacks so far in 2021; Canadian centre says most activity unreported. *National Post*.

Nardi, C. (2021, December 7). Ransomware attacks targeting health, energy sectors; On rise in 2021. *Ottawa Citizen*.

Nardi, C., & Post, N. (2021, December 7). Ransomware attacks targeting health, energy sectors; On rise in 2021. *Ottawa Citizen*.

National NewsMedia Council. (2021). *About Us: Canada's self-regulatory body for news media*. Retrieved from National NewsMedia Council: https://www.mediacouncil.ca/about-us-ethics-journalism/

National Post. (2018, July 13). CRTC uses anti-spam legislation to fine two companies. *National Post*.

National Post News Services. (2018, October 5). Hacking Scandal. *The Ottawa Citizen*.

Nutall, J., & Chiu, J. (2018, December 14). *How a red dot kept Chinese-Canadian readers from getting the full story on Huawei*. Retrieved from The Star: https://www.thestar.com/vancouver/2018/12/14/how-a-red-dot-kept-chinese-canadian-readers-from-getting-the-full-story-on-huawei.html

Nuttall, J. (2018, December 19). Huawei reps lobbied Ottawa's security committee in bid to tell their 'story'. *Toronto Star*.

Nuttall, J. (2018, December 7). Huawei reps lobbied Ottawa's security committee, MPs tied to Beijing in a bid to 'tell their story'. *Toronto Star*.

O'Kane, J. (2021, November 5). RCMP plan to use AI to obtain passwords could threaten privacy rights. *The Globe and Mail*.

O'Kane, J. (2021, November 8). RCMP plan to use AI to obtain passwords could threaten privacy rights. *The Globe and Mail*.

O'Kruk, A. (2018, December 3). Are financial planners taking cybersecurity precautions? To meet new national standards, firms need to ensure clients' information is not put at risk. *The Globe and Mail*.

Organisation for Economic Co-operation and Development. (2010, June 11). *The Evolution of the News and the Internet*. Retrieved from Working Party on the Information Economy: https://www.oecd.org/sti/ieconomy/45559596.pdf

Paddon, D. (2018, October 15). Canada 'Unrealistic' About Cyber-Security; Firms Are Underestimating Threats, Says New Survey. *National Post*.

Paez, B. (2021, July 20). Morning Update: Canada joins allies in condemning China for global Microsoft cyberattacks. *The Globe and Mail*.

Paquette, J. (2018, 11 4). Cybersécurité: un espoir. *Le Droit*.

Parsons, C. (2021, July 15). The new security research rules threaten universities' ability to be open and inclusive. *The Globe and Mail*.

Patel, R. (2021, december 2). Gov. Gen. Mary Simon's office says its internal network was hacked. *Toronto Star*.

Patel, R. (2021, December 3). Governor General's network hacked. *Toronto Star*.

Patterson, K. (2021, July 17). 'Defence' doesn't fit the job of Canada's military any more. Let's create a Department of National Safety instead. *The Globe and Mail*.

Patterson, K. (2021, July 17). The Good Fight. *The Globe and Mail*.

Pearson, M., & Patching, R. (2008). Government media relations: A 'spin' through the literature. *Humanities & Social Sciences papers*, 1-62.

Peesker, S. (2021, October 4). Fraud is up and businesses are the target: Here's how to fight back. *The Globe and Mail*.

Pelley, L. (2021, December 13). *Why omicron is overtaking delta — and what that means for our fight against COVID-19*. Retrieved from CBC News:

https://www.cbc.ca/news/health/why-omicron-is-overtaking-delta-and-what-that-means-for-our-fight-against-covid-19-1.6283611

Proceviat, S. (2018, October 12). Evening Update: U.S. Senators urge Trudeau to block Huawei; Belinda Stronach offered to settle dispute weeks before father's lawsuit; Also: Turkey claims proof missing journalist Jamal Khashoggi was killed. *The Globe and Mail*.

Public Safety Canada. (2018). *National Cyber Security Strategy.* Ottawa: Her Majesty the Queen in Right of Canada.

Public Safety Canada. (2019). *National Cyber Security Action Plan 2019-2024.* Ottawa: Her Majesty the Queen in Right of Canada.

Public Safety Canada. (2020, July 31). *Cyber Security in the Canadian Federal Government*. Retrieved from Cyber Security: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx

Quebec Press Council. (n.d.). *The Council: The Mission*. Retrieved from Quebec Press Council: https://conseildepresse.qc.ca/en/the-council/mission/

Reynolds, C. (2018, October 16). Hackers hit more than 1 in five firms in 2017: StatCan poll. *The Ottawa Citizen*.

Reynolds, C. (2018, October 16). Hackers hit one firm in five in 2017: StatCan; Cyber-Security. *National Post*.

Robertson, D. (2021, December 28). Province fends off rising cyber threats. *Toronto Star*.

Saylor Foundation. (2016). *Mastering Public Relations*. Retrieved from Saylor Foundation: https://saylordotorg.github.io/text_mastering-public-relations/

Schiestel, A. (2018, December 13). The CRTC's spam overreach. *National Post*.

Scholtz, M. (2018, December 26). The Huawei 'Mess". *The Globe and Mail*.

Sehgal, P. (2021, May 6). *Ottawa invests $80 million to support cybersecurity R&D and commercialization*. Retrieved from IT World Canada: https://www.itworldcanada.com/article/ottawa-invests-80-million-to-support-cybersecurity-rd-and-commercialization/447084

Shull, A. (2021, September 20). Canada needs to reimagine security policy. *National Post*.

Silcoff, S. (2017, December 30). Trump, Xi declare progress on U.S.-China trade talks; The world's two largest economies have been in a trade war for much of 2018, shaking world financial markets as tariffs disrupted the flow of hundreds of billions of dollars worth of goods between them. *The Globe and Mail*.

Silcoff, S. (2021, October 6). B.C.'s D-Wave broadens focus. *The Globe and Mail*.

Silcoff, S. (2021, October 6). Once a pioneer, quantum computer developer D-Wave will start making same types of machines as rivals. *The Globe and Mail*.

Silcoff, S. (2021, October 5). Once a pioneer, quantum computer developer D-Wave will start making same types of machines as rivals. *The Globe and Mail*.

Slobodian, S. (2018, October 4). Evening Update: Canada, allies rebuke Russia over alleged hacking; Quebec Liberal leader Couillard retires from politics; Also: U.S. not invited to Canada's save-the-WTO summit of 'like-minded' countries. *The Globe and Mail*.

Slobodian, S. (2018, October 31). Evening Update: Privacy commissioner probing Statscan over efforts to obtain banking records; Canada's economy grows for

seventh straight month; Also: Halifax woman with terminal cancer plans to die tomorrow, saying law is forcing early death on her. *The Globe and Mail*.

Slobodian, S. (2018, December 20). Evening Update: Third Canadian detained in China for working illegally, Beijing says; Ottawa gives Toronto $7-million to combat gangs and guns; Also: Canada can reach Paris emissions target with faster adoption of electric cars, public transit: McKenna. *The Globe and Mail*.

Slobodian, S. (2021, July 19). Evening Update: Ottawa joins allies in denouncing China for cyberattacks; fully vaccinated Americans can travel to Canada starting Aug. 9. *The Globe and Mail*.

Smellie, S. (2021, November 5). Expert says N.L. cyberattack worst in Canadian history, deserves federal response; Health system. *National Post*.

Smith, M.-D. (2018, December 7). PM denies political ties to Huawei arrest; Detaining company's CFO could take a toll on Canada-China relations, experts say. *The Ottawa Citizen*.

Smith, M.-D. (2018, December 7). Trudeau denies political ties to Huawei arrest. *National Post*.

Snider, M. (2018, December 21). Evening Update: Freeland demands China “immediately release” detained Canadians; Also: Fallout over Mattis resignation felt around the world; U.S. prepares for a shutdown over the wall and reviews of Bumblebee, Marwen and Shooting War. *The Globe and Mail*.

Snyder, J. (2021, July 20). China behind massive cyber attack; Canada slams 'harmful behaviour'. *National Post*.

Snyder, J. (2021, July 20). China blamed in microsoft email hack; 400,000 Servers; Biopharm, defence sectors among targeted. *Ottawa Citizen*.

Solbodian, S. (2018, October 31). Evening Update: Privacy commissioner probing Statscan over efforts to obtain banking records; Canada's economy grows for seventh straight month; Also: Halifax woman with terminal cancer plans to die tomorrow, saying law is forcing early death on her. *The Globe and Mail*.

The Canadian Press. (2018, July 13). CRTC Fines Two Companies for Allegedly Violating Anti-Spam Law. *The Globe and Mail*.

The Canadian Press. (2018, July 13). CRTC levies anti-spam fines. *The Ottawa Citizen*.

The Canadian Press. (2018, November 19). Russia Will Meddle in 2019 Vote, Sajjan Warns. *The Globe and Mail*.

The Canadian Press. (2021, November 3). Experts worry about damage to N.L. health system databanks. *The Globe and Mail*.

The Globe and Mail (Breaking News). (2018, December 6). Evening Update: Canada prepared for possible Chinese cyber retaliation over Huawei executive arrest; Hydro One deal for Avista rejected by Washington State; Also: New OPP commissioner bought top Ford staffer's house. *The Globe and Mail*.

The Globe and Mail (Breaking News). (2018, December 6). Evening Update: Canada prepared for possible Chinese cyber retaliation over Huawei executive arrest; Hydro One deal for Avista rejected by Washington State; Also: New OPP commissioner bought top Ford staffer's house. *The Globe and Mail*.

The Globe and Mail (Breaking News). (2018, August 1). Globe editorial: Does Ottawa have a plan to keep our elections safe from meddling? Given the latest Facebook

revelations, the federal government will need a more comprehensive plan to safeguard the 2019 federal vote. *The Globe and Mail*.

The Globe and Mail. (2018, August 2). Social anxieties. *The Globe and Mail*.

The Globe and Mail. (2018, December 15). The end of Canada's China delusion. *The Globe and Mail*.

Thibodeau, M. (2018, October 5). La Russie dénoncée pour une série de cyberattaques. *La Presse*.

Thomson, S. (2018, October 1). 'Privacy is not absolute'; Alarm raised' five eyes'allies want 'backdoor'on tech devices. *National Post*.

Tison, M. (2021, December 13). Mouler du plastique en français. *La Presse*.

Trépanier, A. (2021, December 3). Rideau Hall fait l'objet d'une enquête de cybersécurité. *Le Droit*.

Trépanier, A. (2021, December 2). Rideau Hall fait l'objet d'une enquête de cybersécurité. *Le Droit*.

Trichur, R. (2021, October 12). Banning Huawei from 5G should be first step in assuring. *The Globe and Mail*.

Trichur, R. (2021, October 12). Banning Huawei from 5G should be first step in assuring security. *The Globe and Mail*.

Trichur, R. (2021, October 12). Canada needs a proper technology security strategy. Banning Huawei from 5G should be the first step. *The Globe and Mail*.

Trichur, R. (2021, October 12). Canada needs a proper technology security strategy. Banning Huawei from 5G should be the first step. *The Globe and Mail*.

Tutton, M. (2021, November 2). Suspected N.L. cyberattack hits health network. *National Post*.

Van Wie Davis, E. (2021). *Shadow Warfare: Cyberwar Policy in the United States, Russia, and China.* Lanham, Maryland: Rowman & Littlefield.

Weil, D. (2021, July 19). Microsoft cyberattack came from China, White House says. *Toronto Star*.

Wells, J. (2018, November 2). Jennifer Wells: What one unsettling tale of identity theft can teach Justin Trudeau about data privacy. *Toronto Star*.

Wells, J. (2018, November 3). What identity theft can teach Trudeau. *Toronto Star*.

Whyte, C., & Mazanec, B. (2019). 5 Attack: From exploitation to offensive cyber operations. In C. Whyte, & B. Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy* (p. 83). New York City: Routledge.

Wilner, A. S. (2018). Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation. *International Journal: Canada's Journal of Global Policy Analysis, 73*(2), 308-316.

Zetter, K. (2014). *Countdown to Zero Day.* New York City: Broadway Books.

Zilio, M. (2018, December 31). Australia joins outcry over detention of Canadians in China, but stops short of calling for their release; Foreign Minister Marise Payne did not call for the immediate release of Michael Kovrig and Michael Spavor, despite recent pressure from more than 40. *The Globe and Mail*.

Zillo, M. (2018, December 31). Australia joins outcry over detention of Canadians in China, but stops short of calling for their release; Foreign Minister Marise Payne

did not call for the immediate release of Michael Kovrig and Michael Spavor, despite recent pressure from more than 40. *The Globe and Mail*.

Zimonjic, P. (2021, May 20). *Trudeau says Huawei, ZTE 5G ban took longer because government wanted to get it right*. Retrieved from CBC News - Politics: https://www.cbc.ca/news/politics/trudeau-huawei-ban-cyber-security-1.6461235

Appendix A –Search Terms

English Terms	French Equivalents
Botnet	Botnet
Cybercrime	Cybercriminalité
Cyber Crime	Cyber-criminalité
Cyber Infrastructure	Cyber-infrastructure
Cyber Network	Cyber réseau
Cybersecurity	Cybersécurité
Cyber Security	Cyber-sécurité
Get Cyber Safe	Pensez cybersécurité
Hack	Pirater
Hacked	Piraté
Hacker	Pirate
Hacking	Piratage
Log4j	Log4j
Malware	Malware
NotPetya	NotPetya
Quantum	Quantum
Ransomware	Rançongiciel
Security Event	Événement de sécurité
SolarWinds	SolarWinds
WannaCry	WannaCry

Appendix B – Qualitative Content Analysis Framework

Q1. Item Details: Source, Date, Headline, and Author

Q2. Publication date: 2018 (launch of the National Cyber Security Strategy) or 2021 (current state) with 6-month time ranges from July-December for comparable frames of analysis since the National Cyber Security Strategy was announced on June 12, 2018 (Government of Canada, 2018)

Q3. Perception of Government of Canada response to and actions on cyber security in headlines:

- Positive – Favourable expressions, encouraging qualifiers, or optimistic assessments
- Negative – Disapproving expressions, discouraging qualifiers, or pessimistic assessments
- Neutral – Neither affinity nor deleterious perceptions evidenced, statements of information and facts without obvious biases
- Ambiguous – providing statements, arguments, views, and opinions from proponents of and opposition to the Government of Canada's approach in cyber security without evident political bias towards one side or the other

Q4. Applicable to Positive, Negative, or Ambiguous responses to Q3. What absolutist language is being leveraged to qualitatively frame articles with positive or negative positions on the Government of Canada’s response to and actions on cyber security (e.g., absolutely, completely, naturally, certainly, remarkable, never, unbelievable, disappointing, etc.)? Responses are to be coded with qualifying language as well as its context.

Q5. Perception of Government of Canada response to and actions on cyber security within the abstracts for articles:

- Positive – Favourable expressions, encouraging qualifiers, or optimistic assessments
- Negative – Disapproving expressions, discouraging qualifiers, or pessimistic assessments
- Neutral – Neither affinity nor deleterious perceptions evidenced, statements of information and facts without obvious biases
- Ambiguous – providing statements, arguments, views, and opinions from proponents of and opposition to the Government of Canada's approach in cyber security without evident political bias towards one side or the other

Q6. Applicable to Positive, Negative, or Ambiguous responses to Q5. What absolutist language is being leveraged to qualitatively frame articles with positive or negative positions on the Government of Canada's response to and actions on cyber security (e.g., absolutely, completely, naturally, certainly, remarkable, never, unbelievable, disappointing, etc.)? Responses are to be coded with qualifying language as well as its context.

Q7. Perception of Government of Canada response to and actions on cyber security within the body of articles:

- Positive – Favourable expressions, encouraging qualifiers, or optimistic assessments
- Negative – Disapproving expressions, discouraging qualifiers, or pessimistic assessments

- Neutral – Neither affinity nor deleterious perceptions evidenced, statements of information and facts without obvious biases
- Ambiguous – providing statements, arguments, views, and opinions from proponents of and opposition to the Government of Canada's approach in cyber security without evident political bias towards one side or the other

Q8. Applicable to Positive, Negative, or Ambiguous responses to Q7. What absolutist language is being leveraged to qualitatively frame articles with positive or negative positions on the Government of Canada's response to and actions on cyber security (e.g., absolutely, completely, naturally, certainly, remarkable, never, unbelievable, disappointing, etc.)? Responses are to be coded with qualifying language as well as its context.

Q9. Alignment to Government of Canada's public-facing speaking points and content: Yes or No

Q10. What is the main cyber security concern addressed in the article: Qualitative open-ended responses will be grouped and categorized in compiling the data for analysis (e.g., strategic direction, programs, policies, procurement, international cooperation, public attributions of malicious cyber activity, emerging technology, etc.)?

Q11. Inclusion or awareness of related Government of Canada policies and programs on the article's main subject: Yes or No

Q12. Are links provided to Government of Canada sources: Yes or No

Q13. Department or agency named: Open-ended for organization(s) identified

Q14. Political figures named: Open-ended for political figure(s) identified

Appendix C – 2018 Citations for GC Speaking Points or Content on the Canadian Position on Huawei 5G and Canada's Cyber Security Posture

(Chase & Fife, U.S. senators urge Trudeau to block Huawei from 5G; In letter to PM, two senior committee members warn inadequate safety measures put Canadian national security and 'Five Eyes' joint intelligence, 2018) (Chase & Fife, U.S. senators urge Trudeau to block Huawei from 5G, 2018) (Fife & Chase, U.S. intelligence officials question Canada's ability to test China's Huawei for security breaches; Senior officials reportedly laugh at declaration that Canada possesses sufficient safeguards to address risks posed by telecom giant, 2018) (Fife & Chase, U.S. security officials question Canada's ability to test Huawei risks, 2018) (Chiu & Grauer, Federal government under fire for Canada's Huawei ties, 2018) (Jackson, Huawei arrest puts telecom ties in glare; Canada pressed to re-evaluate relationship, 2018) (Jackson, Huawei exec's arrest puts focus on Chinese company's ties in Canada; Universities with research partnerships say it's business as usual, telecoms mum, 2018) (Chase S. , Canada joins allies in condemning China's hacking campaign, 2018) (Chase, Zillo, & VanderKlippe, Teacher Sarah McIver third Canadian detained in China; Trudeau says doesn't appear to be retaliation for Huawei arrest; Trudeau said details obtained so far suggest this third case is more of a routine matter and different from the Dec. 10 detentions of f, 2018) (Fife & Chase, Five Eyes spy chiefs warned Trudeau twice about Huawei national-security risk; Sources said the spy chiefs stressed that their countries cannot become dependent upon Huawei's 5G technology, 2018) (Fife & Chase, Five Eyes spy chiefs warned Trudeau

twice on Huawei risk, 2018) (Fife & Chase, Trudeau says he knew about the arrest of a top Huawei executive; Meng Wanzhou was picked up by Canadian law enforcement officials in transit at Vancouver airport Dec. 1. at the request of U.S. authorities, 2018) (Fife & Chase, China demands release of Huawei executive, 2018) (Fife, Chase, & Freeze, CSIS chief warns of state-sponsored espionage threat to 5G networks, 2018) (Fife, Chase, & Freeze, CSIS director warns of state-sponsored espionage threat to 5G networks; David Vigneault told a business audience that hostile states are targeting large companies and universities to obtain new technologies, but refrained from naming any particular countr, 2018) (Fife & Chase, New Zealand becomes third Five Eyes member to ban Huawei from 5G network; New Zealand is barring China's Huawei on national-security grounds from supplying equipment for next-generation mobile networks, 2018) (Fife & Chase, New Zealand bans Huawei gear, following U.S. and Australia, 2018) (Fife & Chase, Ottawa not ruling out blocking Huawei from 5G supply contracts; Review under way to determine whether Canada should join the U.S. and Australia in banning Chinese telecommunications giant, Goodale says, 2018) (Fife & Chase, Ottawa reconsiders blocking Huawei from 5G work, 2018) (Fife & Chase, China Telecom diverted internet traffic in U.S. and Canada, report finds; Cybersecurity researchers say state-owned firm has shunted data through legal access points in North America in an effort to steal intellectual property, 2018) (Fife & Chase, Huawei executives lobbied MPs to resist U.S. 5G boycott effort; Representatives of the Chinese telecom began an influence campaign in late August after Australia joined the United States as the second Five Eyes intelligence ally to block the company from , 2018) (Fife & Chase, Huawei lobbies MPs to thwart U.S. 5G boycott effort, 2018) (Chase, Fife, & McKenna, Trudeau defends Huawei policy amid

national security concerns, 2018) (Freeze, Cyber czar says Canada has ‘layers' to protect against potential Huawei threat, 2018) (Freeze, Ottawa’s top cybersecurity official: Canada has ‘layers’ to protect against Huawei threat; Washington has been putting pressure on Canada, Britain and New Zealand to join the United States and Australia in banning Huawei from supplying equipment for the C, 2018) (Hannay & Keller, Politics Briefing: Government workers told to stay home after Ottawa tornado; Also: Trudeau in New York, 2018) (Fife & Chase, No need to ban Huawei, Ottawa says, 2018) (Fife & Chase, No need to ban Huawei in light of Canada’s robust cybersecurity safeguards, top official says; Head of cybersecurity dismisses calls to join U.S. and Australia in blocking Chinese firm, 2018) (Hannay & Keller, Politics Briefing: Canada not making concessions, Republican charges; Also: Ottawa launches cyber security analysis, 2019) (Ligeti, Morning Update: Opioids killing 11 Canadians daily; Facebook shuts down accounts linked to Vancouver election; Also: Ottawa has launched a probe of cyber security, 2018) (Fife & Chase, Ottawa launches probe of cyber security, 2018) (Fife & Chase, Ottawa probes Huawei equipment for security threats; Facing U.S. pressure to ban Chinese firm’s equipment from 5G networks, federal government acknowledges for first time that it has been conducting tests since 2013, 2018) (Fife & Chase, Ottawa probes Huawei devices for security threats, 2018) (Fife, Chase, & Bailey, Trudeau won’t say if Canada will follow Australia, U.S. in blocking Huawei from big projects; The world’s largest maker of telecommunications-network equipment and the No. 3 smartphone supplier, has already been virtually shut out of the U.S. market, 2018) (Fife, Chase, & Bailey, Australia joins U.S. in ban of Huawei from 5G network, 2018) (MacCharles, PM denies role in arrest of Chinese exec; Trudeau says he had 'a few days' notice' of Canada's move to comply with

FBI request, 2018) (Chiu & Grauer, Huawei arrest fuels anxiety over the security of Canada's 5G dealings, 2018) (MacCharles, Trudeau says he had nothing to do with the arrest of Chinese executive in Vancouver, 2018) (Green, 2018) (Codère, 2018) (Fife & Chase, Ottawa launches probe of cyber security; Australia and U.S. have already imposed ban on China's Huawei from participating in new wireless cellular networks, 2018) (The Globe and Mail (Breaking News), 2018) (House, It's About Competition, 2018) (Smith, PM denies political ties to Huawei arrest; Detaining company's CFO could take a toll on Canada-China relations, experts say, 2018) (Zillo, 2018) (Scholtz, 2018) (Dobby, Bell, Telus warn of 5G delays, higher costs if Ottawa joins peers in banning Huawei; They argue that security concerns related to Huawei can be addressed by testing its equipment and restricting its gear to non-sensitive parts of their networks, 2018) (Chase, Zilio, & VanderKlippe, 2018) (Fife & Chase, Ottawa sees Chinese-owned Huawei as major security threat, senior officials say; Trudeau government and allies alarmed by high-tech giant's growing dominance in 5G telecommunications technology, 2018) (Fife & Chase, Ottawa's worries grow over global ambitions of Huawei, 2018) (Nuttall, Huawei reps lobbied Ottawa's security committee in bid to tell their 'story', 2018) (Nuttall, Huawei reps lobbied Ottawa's security committee, MPs tied to Beijing in a bid to 'tell their story', 2018) (Smith, Trudeau denies political ties to Huawei arrest, 2018)

Appendix D – 2018 Citations for GC Policy and Programs related to Huawei 5G Including the Cyber Security Review and Testing Facilities for Telecommunications Technologies Backdoors

(Chase & Fife, U.S. senators urge Trudeau to block Huawei from 5G; In letter to PM, two senior committee members warn inadequate safety measures put Canadian national security and 'Five Eyes' joint intelligence, 2018) (Chase & Fife, U.S. senators urge Trudeau to block Huawei from 5G, 2018) (Fife & Chase, U.S. intelligence officials question Canada's ability to test China's Huawei for security breaches; Senior officials reportedly laugh at declaration that Canada possesses sufficient safeguards to address risks posed by telecom giant, 2018) (Fife & Chase, U.S. security officials question Canada's ability to test Huawei risks, 2018) (Chiu & Grauer, Federal government under fire for Canada's Huawei ties following arrest in Vancouver, 2018) (Jackson, Huawei arrest puts telecom ties in glare; Canada pressed to re-evaluate relationship, 2018) (Jackson, Huawei exec's arrest puts focus on Chinese company's ties in Canada; Universities with research partnerships say it's business as usual, telecoms mum, 2018) (Zilio, 2018) (Dobby, Bell, Telus warn of 5G delays, higher costs if Ottawa joins peers, 2018) (Chase, Zilio, & VanderKlippe, Detention of third Canadian doesn't appear to be tied to Huawei, PM says, 2018) (Chase, Zilio, & VanderKlippe, Teacher Sarah McIver third Canadian detained in China; Trudeau says doesn't appear to be retaliation for Huawei arrest; Trudeau said details obtained so far suggest this third case is more of a routine matter and different from the Dec. 10 detentions of f, 2018) (Fife & Chase, Five Eyes spy chiefs warned Trudeau twice about Huawei national-security risk; Sources said

the spy chiefs stressed that their countries cannot become dependent upon Huawei's 5G technology, 2018) (Fife & Chase, Five Eyes spy chiefs warned Trudeau twice on Huawei risk, 2018) (Fife & Chase, New Zealand becomes third Five Eyes member to ban Huawei from 5G network; New Zealand is barring China's Huawei on national-security grounds from supplying equipment for next-generation mobile networks, 2018) (Fife & Chase, New Zealand bans Huawei gear, following U.S. and Australia, 2018) (Fife & Chase, Ottawa not ruling out blocking Huawei from 5G supply contracts; Review under way to determine whether Canada should join the U.S. and Australia in banning Chinese telecommunications giant, Goodale says, 2018) (Fife & Chase, Ottawa reconsiders blocking Huawei from 5G work, 2018) (Fife & Chase, China Telecom diverted internet traffic in U.S. and Canada, report finds; Cybersecurity researchers say state-owned firm has shunted data through legal access points in North America in an effort to steal intellectual property, 2018) (Fife & Chase, Huawei executives lobbied MPs to resist U.S. 5G boycott effort; Representatives of the Chinese telecom began an influence campaign in late August after Australia joined the United States as the second Five Eyes intelligence ally to block the company from , 2018) (Fife & Chase, Huawei lobbies MPs to thwart U.S. 5G boycott effort, 2018) (Chase, Fife, & McKenna, Trudeau defends Huawei policy amid national security concerns, 2018) (Freeze, Cyber czar says Canada has 'layers' to protect against potential Huawei threat, 2018) (Freeze, Ottawa's top cybersecurity official: Canada has 'layers' to protect against Huawei threat; Washington has been putting pressure on Canada, Britain and New Zealand to join the United States and Australia in banning Huawei from supplying equipment for the C, 2018) (Hannay & Keller, Politics Briefing: Government workers told to stay home after Ottawa tornado; Also: Trudeau in

New York, 2018) (Fife & Chase, No need to ban Huawei, Ottawa says, 2018) (Fife & Chase, No need to ban Huawei in light of Canada's robust cybersecurity safeguards, top official says; Head of cybersecurity dismisses calls to join U.S. and Australia in blocking Chinese firm, 2018) (Hannay & Keller, Politics Briefing: Government workers told to stay home after Ottawa tornado; Also: Trudeau in New York, 2018) (Ligeti, Morning Update: Opioids killing 11 Canadians daily; Facebook shuts down accounts linked to Vancouver election; Also: Ottawa has launched a probe of cyber security, 2018) (Fife & Chase, Ottawa probes Huawei equipment for security threats; Facing U.S. pressure to ban Chinese firm's equipment from 5G networks, federal government acknowledges for first time that it has been conducting tests since 2013, 2018) (Fife & Chase, Ottawa probes Huawei devices for security threats, 2018) (Green, 2018) (Fife & Chase, Ottawa launches probe of cyber security; Australia and U.S. have already imposed ban on China's Huawei from participating in new wireless cellular networks, 2018) (House, It's About Competition, 2018) (Jackson, Huawei pledges cyber security; 5G Networks; 'Whatever'Canada requires, China giant says, 2018) (Silcoff, Trump, Xi declare progress on U.S.-China trade talks; The world's two largest economies have been in a trade war for much of 2018, shaking world financial markets as tariffs disrupted the flow of hundreds of billions of dollars worth of goods between them, 2017) (Fife & Chase, Huawei chairman challenges security risk concerns, demands proof that tech giant is a pawn of Beijing; Huawei chairman warned that banning Huawei from supplying next-generation 5G mobile technology to Western countries would raise costs to consumers and s, 2018) (Fife & Chase, Huawei chairman challenges security risk concerns, demands proof that tech giant is a pawn of Beijing, 2018) (Ligeti, Morning Update: Charges stayed in major B.C.

money-laundering case; another Five Eyes ally bars Huawei from 5G;, 2018) (Proceviat, 2018) (Hannay & Keller, Politics Briefing: The new trade deal is here; Also: Quebec votes today, 2018)

Appendix E – Database of Articles Consulted

Please see Major Research Paper Database of Records for the complete database of articles consulted with associated dispositions per this research.