Cybersecurity and Critical Infrastructure: An Analysis Using Securitization Theory

Noah T Archibald, Acadia University, Wolfville, Nova Scotia, Canada

Abstract

This paper will analyze current insecurities in Canada's critical infrastructure and the ways these insecurities have been justified as warranting additional protections. Namely, examples of threats posed by foreign state-sponsored hackers, cyber-terrorism campaigns, and the company: Huawei will be analyzed. Each of these three examples will be examined using a post-positive approach with qualitative data and some use of quantitative data. The Copenhagen School approach is utilized as a theoretical framework of analysis through securitization theory. A meta-analysis is conducted to understand past theoretical and empirical approaches to critical infrastructure. This paper will ask how national and international uses of discourses, policy, and legislation concerning these three areas have contributed to the larger securitization of Canadian critical infrastructure.

It is argued that the securitization of critical infrastructure in Canada as a cybersecurity concern has been as a result of numerous speech acts, executive orders, and uses of discourse by a variety of state and non-state actors. The hypothesis under analysis finds a causal relationship between the use of such discourses, policies, and legislation on how cybersecurity is interpreted as a national security concern.

Keywords: Securization, Copenhagen School, critical infrastructure, state-sponsored hackers, cyber-terrorism, Huawei, national security, Canada

Cybersecurity and Critical Infrastructure: An Analysis Using Securitization Theory

Critical infrastructure is defined by Public Safety Canada as being the "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government" (Public Safety Canada, 2019, par. 1). Canada's critical infrastructure enables mass communication networks, water supply, finance and banking, natural gas, transportation, and power grids. As Canadian citizens and the Canadian state remain structurally dependant on critical infrastructure for economic, political, and societal needs, there has been increased pressure to implement additional security measures for improved protection.

The Copenhagen School framework will be utilized to examine three instances that have experienced securitizing discourse. The Copenhagen School utilizes securitization theory to consider how political issues are characterized as matters concerning safety and security in efforts to remove them from the realm of public debate. More specifically, securitization theory examines how state and non-state actors utilize discourse, speech acts, legislation, and executive orders to designate an issue as a threat. Speech acts function as a broad form of discourse which both presents information and acts to securitize an issue. Within the context of this paper, issues will be analyzed in relation to how they have been characterized as cybersecurity issues. Cybersecurity is specifically the realm of securitization, which is concerned with computer systems, the internet, electronic hardware, software, and critical infrastructure. Three areas of risk which have been characterized as a threats to critical infrastructure will be analyzed. Cyber-terrorism, state-sponsored hacking, and Huawei are relevant areas of analysis as they concern recent developments which are essentially connected to the securitization of critical infrastructure.

Cyber-terrorism acts as a relevant area of examination in relation to the securitization of Canadian infrastructure as it has been frequently referenced by both state and non-state actors as an issue which concerns national security. Cyber-terrorism is differentiated from other forms of insecurity in that it is conducted by non-state actors for political, social, or religious causes (Kenney, 2015). What differentiates cyber-terrorism from other areas of analysis is that it specifically concerns actions taken by non-state actors against critical infrastructure. Historically, cyber-terrorism efforts have targeted Supervisory Control and Data Acquisition (SCADA) systems that regulate and control critical infrastructure (Kenney, 2015).

The subject of state-sponsored hackers has increased over recent years with the projected number of state hackers expected to increase into the future (Nguyen, 2015). This area has become increasing relevant due to media coverage in recent years as a result of foreign election interference. Notable states have begun utilizing state-sponsored hackers which include Russia, North Korea, China, Indonesia, and the United States (Nguyen, 2015; Vincent, 2017). As discourse relating to recent interference by state-sponsored hackers in elections continues to be a major political focus in Canada, this subject be analyzed in detail.

Warnings against potential dangers that the company Huawei pose have spread increasingly over the past year with warnings from security officials and experts (Braga, 2019). Much of this is as a result of increased discussion of 5G technology implementation into Canada's telecommunications network. The American government has banned the company from the United States, citing alleged links to the Chinese state and military, and has warned other Five Eyes states to do the same or risk losing access to American classified intelligence (Harnik, 2019). The Five Eyes is an intelligence alliance between the United States, Canada, New Zealand, Australian, and the United Kingdom. As the alliance allows all five states to actively share classified information among one another, recent discourse by American state

actors threaten its future. Huawei acts as an important area of analysis as it relates more broadly to potentially restricting business access to Canada as a result of conceptualizing critical infrastructure as a national security issue.

In this research paper, it is argued that the securitization of Canadian critical infrastructure as a cybersecurity concern has been as a result of speech acts, policies, legislation, and discourse by a variety of actors. It will be examined how the global use of discourses, policies, and legislation have contributed to the larger securitization of Canadian critical infrastructure within a global context. The Copenhagen School approach will be utilized through a comprehensive meta-analysis to ask how national and international uses of discourses, policies, and legislation have contributed to the securitization of critical infrastructure in Canada.

This paper will be made up of a methods section, literature review, analysis, and conclusion. The methods section will outline the framework of analysis. The literature review will comprise of identifying academic texts which are relevant and summarizing their approaches. The literature review will also analyze how the arguments presented in applicable sources differ and contrast to other research. Later analysis will examine evidence in-depth. The conclusion will act as a reflection of this research and detail how future studies could expand on the subject of critical infrastructure and cybersecurity.

Methods

This study will utilize a meta-analysis to better understand both past and present theoretical and empirical approaches to cybersecurity and its relation to critical infrastructure. This section will outline the methods of examining existent academic research in the literature review while also providing an outline of the framework used in the later analysis of this paper.

As the study into critical infrastructure is vast and broad, the study of secondary sources in the literature review will span over the past fifteen years to ensure appropriate timely

relevance. It will also focus on Canadian critical infrastructure and that of member states in the Five Eyes intelligence alliance. By utilizing cases by Five Eyes states, the scope of global securitization can be understood in relation to Canada's critical infrastructure. These parameters of research will establish proper context on existing research and arguments within the field of critical infrastructure.

As this paper argues that securitization of critical infrastructure comes as a result of speech acts and policies used by actors, the analysis will focus on qualitative examples with some additional quantitative analysis. Data collection will be centered on observed events that have led to the securitization of critical infrastructure. There will be analysis of legislation, speeches, and government documents. Analysis will include, but not be limited to, Government of Canada webpages, publicized documents, and speeches. There will also be some empirical analysis and examination of government spending patterns. Budget documents from the Canadian Department of Finance will be utilized. Relevant findings from existing academic articles will also be included. News articles from reputable sources will be referenced. Analysis will use a post-positivist approach to justify the relation of discourse on securitization. Post-positivism is a theoretical stance which examines various perspectives to understand existing power relations in international relations. It is an approach which recognizes the existent of biases in research as it is impossible to be fully independent.

The analysis of this paper will be comprehensive yet intellectual by targeting scholars and students as the audience. This research paper will distinguish itself among previously written works in its analysis of critical infrastructure through the theoretical framework of the Copenhagen School approach by analyzing concerns of cyber-terrorism, state-sponsored hackers, and Huawei.

Literature Review

Empirical and scientific based approaches to understanding cyber-insecurities are often utilized in texts that seek to identify vulnerabilities in current critical infrastructure. These texts often resort to mathematical and scientific reasoning. This can be seen in Roy, Ellis, Shiva, Dasgupta, Shandilya, and Wu's (2010) "A Survey of Game Theory as Applied to Network Security" that uses the empirically informed game theory to examine how actors interact. "A Survey of Game Theory as Applied to Network Security" understands how the effectiveness of efforts to increase cybersecurity are contingent on actions that are taken to threaten it (Roy et al., 2010). This use of game theory illustrates actor dynamics in global politics but prove ineffective at generating a more comprehensible understanding for readers who are unfamiliar with the concepts.

Ralston, Graham, and Hieb's (2007) "Cyber-Security Risk Assessment for SCADA and DCS Networks" utilizes a unique empirical approach. They agree that focus should be emphasized on understanding the risk, probability, and potential impact of an attack but they instead choose to use attack and vulnerability trees to analyze these probabilities (Ralston et al., 2007). This scientific form of analysis continues in the tradition of other sources who use scientific methods to understand the level of threats to critical infrastructure systems. Ted Lewis' (2006) "Critical Infrastructure in Homeland Security: Defending a Networked Nation" examines the extent of connection between networks and attempts to identify possible weaknesses. This is done using network theory and simulation software which are both scientifically informed (Lewis, 2006). These previously noted texts are similar in their focus on reducing risk of cybersecurity attack.

Many sources instead choose to use qualitative and historical analysis to understand the role of cybersecurity on critical infrastructure. Cox's (2013) "Canada and the Five Eyes

Intelligence Community" argues that states which are participants of the Five Eyes intelligence alliance should improve critical infrastructure security to ensure secure intelligence sharing to other states in the intelligence alliance. Another example of a source that utilizes qualitative data is that of Vincent's "State-Sponsored Hackers: The New Normal for Business". Vincent (2017) uses historical examples such as recent foreign election interference and data breaches to argue that state-sponsored hackers are becoming more prevalent. He argues that governments and businesses should adapt to secure networks. Similarly, Shoebridge's (2018) "Chinese Cyber Espionage and the National Security Risks Huawei Poses to 5G Networks" relies on qualitative data in the form of historical events and law to explain the context of the technology company, Huawei. Shoebridge (2018) explains how Huawei could pose potential threats to Canada's critical infrastructure. Although most texts focus on the American state as an example, Shoebridge and Cox are two of the few sources that focuses specifically on the Canadian state's critical infrastructure. Arguments presented by Cox, Vincent, and Shoebridge have a common theme which legitimize and support increased funding for critical infrastructure security.

Nguyen's analysis, in "State Sponsored Hacking and Espionage", is very unique in that it utilizes a balanced combination of both qualitative and quantitative data. Nguyen (2015) examines statistics to examine the number of hackers by state while also utilizing historical information to document successful state-sponsored hacking attacks.

As a result of many texts focusing on the effects of attempts by actors to stabilize and destabilize western critical infrastructure, this contributes to a larger western-centric view across all texts examining cybersecurity. This has its consequences in that it reinforces understandings of internal security and external threats but is likely done unintentionally. As critical infrastructure has been characterized as a national security issue, the format of cybersecurity

analysis is often forced into a predetermined western framework. It should be noted that this can unintentionally exclude other perspectives and reiterate western-centric binaries.

Many academic texts differ in who they select as their target audience. Many scientifically informed texts are often aimed at use for professionals. Lewis' methods are used to educate business professionals and policymakers in ways to secure American infrastructure from external threats. This can be seen in how he promotes the allocation of scarce resources to areas that minimize risk (Lewis, 2006). Differing from this approach, other sources attempt to communicate to academics and scholars. Hansen and Nissenbaum's (2009) "Digital Disaster, Cyber Security, and the Copenhagen School" is an example of this as they critique past actions by the state, businesses, and the media.

The majority of studies to date, with the exception of Hansen and Nissenbaum's "Digital Disaster, Cyber Security, and the Copenhagen School," do not use the Copenhagen School to explain the securitization of critical infrastructure. Hansen and Nissenbaum's analysis diverges from earlier interpretations of cybersecurity in its use of the Copenhagen School to explain how critical infrastructure has been securitized as a result of discourse. Hansen and Nissenbaum's (2009) analysis also distinguishes itself in how it looks mainly at internal western actors who have securitized the issue of cybersecurity. They seldom consider how external actors have the ability to harm critical infrastructure. Instead, Hansen and Nissenbaum resort to examining the role of discourse by state and business actors. This can be seen in their analysis of 'if-then' rhetoric which is used to justify increased critical infrastructure securitization (Hansen & Nissenbaum, 2009).

Analysis

The concept and common use of cybersecurity was originally introduced in the early 1990s by computer scientists to illustrate potential risks associated with using computers

(Hansen & Nissenbaum, 2009). They originally referred to it as being ‘computer security’ but that term was later replaced with ‘cybersecurity’ by American politicians, private corporations, and the media (Hansen & Nissenbaum, 2009). The term has been used to reference attaining a state of security in relation to electronic networks, hardware, software, and critical infrastructure but is instead indicative of securitization within the context of this paper. Many of these actors warned of “weapons of mass disruption” (Hansen & Nissenbaum, 2009, p. 1155) and future “electronic Pearl Harbors” (Hansen & Nissenbaum, 2009, p. 1155) to legitimize the use of computers as a security issue. Following 9/11, there has been increased attention into potential cyber-vulnerabilities in networks and critical infrastructure. Examples of discourses surrounding state-sponsored hackers, cyber-terrorism, and the securitization of Huawei have increased in relevancy since 9/11 and will be used to further establish the securization of Canada’s critical infrastructure.

Cyber-Terrorism

Cyber-terrorists can be defined as non-state actors which threaten existing networks, hardware, software, or critical infrastructure. As a result of focus on terrorist threats in recent years by governments and media organizations, discourse relating to cyber-terrorists has led in-part to the characterization of critical infrastructure as a national security concern.

Cyber-terrorism attempts against Canada have existed before the late 2000s but received increased attention by Canadian Prime Minister Stephen Harper. In 2010, Stephen Harper had Governor General Michaëlle Jean deliver his throne speech in the senate chamber (Canadian Governor General, 2010). In this speech he described how terrorists threatened the country’s national security and were “real, significant, and shifting threats” (Canadian Governor General, 2010, p. 14). He stressed the importance of enacting legislation that would protect infrastructure from terrorists (Canadian Governor General, 2010). Two years later, then-US Defense Secretary

Leon Panetta warned that vulnerabilities in American critical infrastructure could allow extremist groups to derail trains, contaminate water supplies, and shutdown power grids (Kenney, 2015). He explained that such an attack could lead to a "cyber Pearl Harbour" (Kenney, 2015, p. 111).

Following Stephen Harper's throne speech, his government released the first ever *Cyber Security Strategy* (Public Safety Canada, 2018). In 2018, Justin Trudeau's liberal government enacted the updated *National Cyber Security Strategy* which addressed issues of "[criminals] and other malicious cyber threat actors" (Public Safety Canada, 2018, p. 2) and warned of how they "disrupt and sometimes destroy the infrastructure that we rely on for essential services and our way of life" (Public Safety Canada, 2018, p. 2).

These speech acts and enactments of policy demonstrate a successful portrayal of critical infrastructure as a referent object. This comes as a result of portraying cyber-terrorism as a national security concern. The use of Leon Panetta's 'if-then' narrative contributed to securitizing critical infrastructure as something in need of additional state protection due to possible threats. The prominence of cybersecurity and critical infrastructure within the federal government and department of Public Safety Canada is indicative of a causal relationship between this use of speculative discourse and eventual construction of cyber issues as security problems.

State-Sponsored Hackers

State-sponsored hackers can be defined as computer experts which act on behalf of a state to accomplish political interests through technological means. They present relevance as they are often presented as threats to critical infrastructure by foreign states. The usage of state-sponsored hackers has become a prevalent practice in recent decades with prominent campaigns such as Shady RAT, Red October, Flame, PRISM, Sony Pictures, and Stuxnet (Nguyen, 2015). Although

these respective campaigns experienced securitizing discourse in response, recent use of state-sponsored hackers in western elections remain a current example of state-sponsored hacking.

Following recent election interference by Russian state-hackers in the 2016 Brexit referendum, the 2016 American presidential election, and the 2017 French presidential election, there was increased attention by the media and politicians on state-sponsored hackers and their ability to interfere in foreign elections (Sanchez, 2018; Vincent, 2017). Following election interference, affected state governments, with the exception of the Trump Administration, agreed to cooperate with intelligence and security services (Sanchez, 2018). Security and intelligence agencies, including the NSA, have confirmed that Russian state-hackers affected foreign elections and that there should be increased protections in place to secure future elections (Sanchez, 2018).

Following this recent interference, many actors have speculated on possible interference in Canadian elections. Former NATO researcher, Janis Sarts, warned of possible attempts by state-sponsored hackers to affect Canada's electoral process (Blanchfield, 2018). He has conducted interviews and testified before the US Senate intelligence committee (Blanchfield, 2019).

This use of speech acts and media attention has led to increased funding towards cybersecurity. Before major election interference, the 2015 Canadian budget allocated 58 million dollars over five years to "protect the Government of Canada's essential cyber systems and critical infrastructure against cyber attacks." (Government of Canada, 2015, par. 7). An additional 36.4 million dollars was allocated to operators of cyber systems (Government of Canada, 2015). In the 2018 Canadian budget, funding was drastically increased with 507.7 million dollars being allocated towards cybersecurity (Department of Finance, 2018). This

demonstrates a relative increase of 413 million dollars of variation between respective budgets since election interference.

These speech acts and other forms of speculative security logic have successfully characterized issues of cybersecurity and critical infrastructure as national security concerns. Speculative security discourse has justified additional state involvement and emergency measures, as seen in Canada's budget in 2018. External cases of state-sponsored hacking in other states have been used to justify action taken by the Canadian state to securitize critical infrastructure as the result of hypothetical rhetoric and analysis.

Huawei

Securitization of the company Huawei as a national security concern has arisen over recent years as a result of its expansion into western markets and proposals to build 5G networks in Canada and other countries. Huawei is a Chinese tech company which specializes in both software and hardware development. 5G stands for fifth edition cellular network technology and its development would upgrade current critical infrastructure to accommodate faster wireless speeds. As implementation of a 5G network in Canada would allow Huawei to have direct access to the Canada's critical infrastructure, US intelligence officials and politicians have warned about risks associated with using the company's technology (Braga, 2019). This stems from allegations that the company is too close with the Chinese state and that the company could leak classified intelligence travelling through the infrastructure. The United States government has banned Huawei from the country and has accused the company of bank and wire fraud, obstructing justice, and conspiring to steal trade secrets (Braga, 2019). US Secretary of State, Mike Pompeo, has warned that states that allow Huawei to integrate technology into their critical infrastructure will not be permitted to access American classified information (Harnik, 2019). This warning threatens the existence of the Five Eyes intelligence alliance. At the end of 2018

and beginning of 2019, many telecom companies internationally announced that they will not utilize Huawei technology in their telecommunications infrastructure (Braga, 2019).

As it currently stands, the Canadian state has not banned Huawei from implementing 5G technology in Canadian critical infrastructure. It should also be noted that experts have speculated that the Canadian government has delayed banning the network as a result of recent tensions between the Canadian and Chinese states internationally (Wingrove, 2019). Although additional action by the Canadian state has not yet been taken to ban the company, international narratives and bans have already justified taking such action as a national security concern. The basis for banning Huawei through the justification of national security is already justified as a result of the ban by the United States and the discourse maintained by Secretary of State Mike Pompeo. Policy and speech acts by predominantly outside actors have justified emergency measures that can be used to protect Canadian critical infrastructure networks in a similar manner to measures already taken by other states.

Conclusion and Further Study

This paper finds that, as a result of discourse and speech acts surrounding cyber-terrorism, state-sponsored hackers, and Huawei, Canada's critical infrastructure has been consequently securitized and characterized as an issue concerning national security. This is evident through Canadian government reports, budget spending, and discourse. The characterization of critical infrastructure as a national security concern comes as a result of anticipatory rhetoric which use "if-then" statements as justification for improved protections. As cyber-terrorism, state-sponsored hackers, and Huawei have been identified as legitimate threats to critical infrastructure, Canada's critical infrastructure is now recognized as something which requires additional state protection.

As the realm of security studies continues to evolve and expand, this insight adds a new perspective on understanding critical infrastructure by utilizing the Copenhagen School through securitization theory. As existing literature has not largely considered securitizing discourse in instances of cyber-terrorism, state-sponsored hackers, and Huawei, this article introduces new research which can continue to be studied and developed. As a result of limitations to the extent of this research, there are many areas of critical infrastructure which can be expanded in increased detail. Although the research presented in this paper justifies how Canada's critical infrastructure has been securitized, it does not go into detail about the political and social consequences of securitizing critical infrastructure as a national security concern.

Further research should elaborate on the consequences that arise from the securitization of critical infrastructure. As critical infrastructure has been securitized, how does this impact rights and freedoms? As successful securitization of an issue results in its removal from the realm of political debate, the effects of this change should be analyzed in further detail. Future research could examine the in-depth changes to governmental policy and how these changes in policy have affected political society and future discourse. The role of discourse in securitization should be further researched to better understand which actors benefit from the securitization of critical infrastructure and which actors are negatively affected.

Further directions of analysis should also consider the effects of the possible westernization of critical infrastructure. Researchers could examine how understanding critical infrastructure as a national security concern has or has not perpetuated existent binaries in security studies.

As with any research project, it is necessary to exclude some details. These exclusions provide future possibilities of analysis surrounding the concept of critical infrastructure and cybersecurity that can grow the topic in coming years.

References

Blanchfield, M. (2018, February 27). NATO researcher warns of Russian interference in 2019 Canadian election. *Globe and Mail.* Retrieved from https://www.theglobeandmail.com/news/politics/nato-researcher-warns-of-russian-interference-in-2019-canadian-election/article38124979/

Braga, M. (2019, January 30). If Huawei were a security risk, how would we find out? *CBC News.* Retrieved from https://www.cbc.ca/news/technology/huawei-5g-security-testing-vulnerabilities-risks-proof-ban-1.4997957

Canadian Governor General. (2010). *Speech from the Throne*. Retrieved from http://publications.gc.ca/collections/collection_2010/bcp-pco/SO1-1-2010-eng.pdf

Cox, J. (2012, December 18). Canada and the five eyes intelligence community. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.357.5576&rep=rep1&type=pdf

Department of Finance. (2018). Equality growth: A strong middle class. Retrieved from https://www.budget.gc.ca/2018/docs/plan/budget-2018-en.pdf

Government of Canada. (2015). Protecting Canadians. Retrieved from https://www.budget.gc.ca/2015/docs/plan/ch4-3-eng.html

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175. doi: 10.1111/j.1468-2478.2009.00572.x

Harnik, A. (2019, February 21). Mike Pompeo says U.S. won't partner with countries that use Huawei systems. *Globe and Mail*. Retrieved from https://www.theglobeandmail.com/business/international-business/us-business/article-mike-pompeo-says-us-wont-partner-with-countries-that-use-huawei/

Kenney, M. (2015). Cyber-terrorism in a post-stuxnet world. *Orbis, 59*(1), 111-128. doi: 10.1016/j.orbis.2014.11.009

Lewis, T. G. (2006). *Critical infrastructure protection in homeland security: defending a networked nation*. Hoboken, NJ: John Wiley & Sons. doi:10.1002/0471789542

Nguyen, D. (2015). State sponsored cyber hacking and espionage. *Infosec Writers*. Retrieved from https://infosecwriters.com/Papers/DNguyen_State_Sponsored_CyberHacking_and_Espionage.pdf

Public Safety Canada. (2019). Critical infrastructure. Retrieved from https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

Public Safety Canada. (2018). National cyber security strategy. Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-en.pdf

Ralston, P., Graham, J., and Hieb, J. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions, 46*(4), 583-594. doi: 10.1016/j.isatra.2007.04.003

Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., & Wu. Q. (2010). A survey of game theory as applied to network security. In R. H. Sprague (Ed.), *43rd Hawaii International Conference on System Sciences* (pp. 1-10). Washington DC: IEEE Computer Society. doi: 1-10. 10.1109/HICSS.2010.35

Sanchez, L. G. (2018). Russian meddling in western elections, 2016-2017: A preliminary probe (Master's thesis, Texas State University, San Marcos, Texas). Retrieved from https://digital1.library.txstate.edu/bitstream/handle/10877/7482/LOPEZSANCHEZ-THESIS-2018.pdf?sequence=1&isAllowed=y

Shoebridge, M. (2018). Chinese cyber espionage and the national security risks Huawei poses to 5G networks. *MacDonald-Laurier Institute Publication*. Retrieved from http://macdonaldlaurier.ca/files/pdf/MLICommentary_Nov2018_Shoebridge_Fweb.pdf

Vincent, A. (2017). State-sponsored hackers: the new normal for business. *Network Security, 2017*(9), 10-12. doi: 10.1016/s1353-4858(17)30113-7

Wingrove, J. (2019, February 6). Huawei likely faces 5G ban in Canada, security experts say. *Financial Post.* Retrieved from https://business.financialpost.com/telecom/huawei-likely-faces-5g-ban-in-canada-security-experts-say