National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

HUAWEI AND THE 5G THREAT: CANADIAN STATUTES, TREATY PROVISIONS AND POLICIES TO PROTECT CANADA'S NATIONAL SECURITY

Major Matthew Maxwell

JCSP 46

Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 46

Solo Flight

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 46 – PCEMI 46

2019 – 2020

SOLO FLIGHT

HUAWEI AND THE 5G THREAT: CANADIAN STATUTES, TREATY PROVISIONS AND POLICIES TO PROTECT CANADA'S NATIONAL SECURITY

By Major Matthew Maxwell

Word Count: 5,257

Nombre de mots : 5.257

HUAWEI AND THE 5G THREAT: CANADIAN STATUTES, TREATY PROVISIONS AND POLICIES TO PROTECT CANADA'S NATIONAL SECURITY

INTRODUCTION

The Chinese Government has been pursuing a strategy to build its economic and technological base to become a more powerful nation.[1] Their aim to build an economic and technological base is evident through the Belt and Road Initiative (BRI), and the rapid increase in Chinese research and development (R&D)[2], respectively. Chinese companies are becoming global leaders in technology, but some nations see China's rapid development and expansion as a threat to their national security.[3] For Huawei, this has played out very publically on the international stage as some states are claiming that Huawei's access to their fifth generation (5G) network would pose a threat to their national security.[4]

The Government of Canada (GoC) has not yet made a decision as to whether they will allow Huawei access to Canada's 5G network, and a national security review is currently underway to assess the national security risks associated with Canada's 5G network.[5] The purpose of this paper is to examine how existing Canadian statutes, treaty provisions and GoC policies might shape and influence the GoC's decision to either allow, or deny, Huawei access to Canada's 5G network. This paper focuses solely on the intersection of existing statutes, treaty provisions, and policy documents, and does not analyze political or economic

---

[1] Phillip C. Saunders, "China's Global Activism: Strategy, Drivers and Tools." *Institute for National Strategic Studies,* Occasional Paper 4 (October 2006): 1.

[2] Forbes, China is Closing the Gap with the U.S. in R&D Expenditure, last accessed 27 April 2020, https://www.forbes.com/sites/niallmccarthy/2020/01/20/china-is-closing-the-gap-with-the-us-in-rd-expenditure-infographic/#1b51b1135832

[3] New York Times, "Trump Officials Battle Over Plan to Keep Technology Out of Chinese Hands", last accessed 27 April 2020, https://www.nytimes.com/2019/10/23/business/trump-technology-china-trade.html

[4] US Department of Commerce, "Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List – Docket No, 190814-0013 Federal Register Vol 84, No 162, (Bureau of Industry and Security, Commerce: 2019).

[5] Public Safety, "Fifth Generation Wireless Technology (5G)", last accessed 1 April 2020, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/031/index-en.aspx

considerations. It is acknowledged that a decision made by the GoC will balance the political and economic considerations against any other considerations as they can never be divorced from a decision. The goal is to determine the space in which decision-making can occur, not whether or not a particular decision will be made, or how politics and economics will intersect with the decision-making space.

In the first section of this paper, a brief introduction to the concept of national security is provided, and is followed by a short description of 5G technology, Huawei, and why the GoC may consider Huawei's involvement in its 5G network to be a potential threat to national security. In the subsequent section, the decisions made by Canada's closest allies on allowing, or denying, Huawei access to their 5G networks will be presented in order to help define the potential solution space. This will be followed by a discussion of the existing Canadian statutes, treaty provisions and GoC policies that may enable or constrain the GoC's decision to allow, or deny, Huawei access to its 5G network. Based on the analysis, it will be shown that existing Canadian statutes, treaty provisions, and GoC policies will enable the GoC to restrict Huawei's access, as required, to mitigate potential threats to national security.

NATIONAL SECURITY

A legal definition of national security is not found in the *National Security Act*,[6] the *National Security and Intelligence Committee of Parliamentarians Act*,[7] or any other Canadian statute.[8] In 2004, Canada released its national security policy which states that national security "deals with threats that have the potential to undermine the security of the

[6] National Security Act, S.C., c. 13, (2019).
[7] National Security and Intelligence Committee of Parliamentarians Act, S.C., c.15, (2019).
[8] National Security and Intelligence Committee of Parliamentarians, *Annual Report 2018* (Ottawa: National Security and Intelligence Committee of Parliamentarians, 2019), 17.

state or society. These threats normally require a national level response…"[9] The policy also provided a Venn diagram, see Figure 1, which depicts how the GoC interprets the interactions between national security, personal security and international security, in addition to what types of threats fall under those categories. It is noteworthy, that both espionage and critical infrastructure are considered under the national security umbrella.

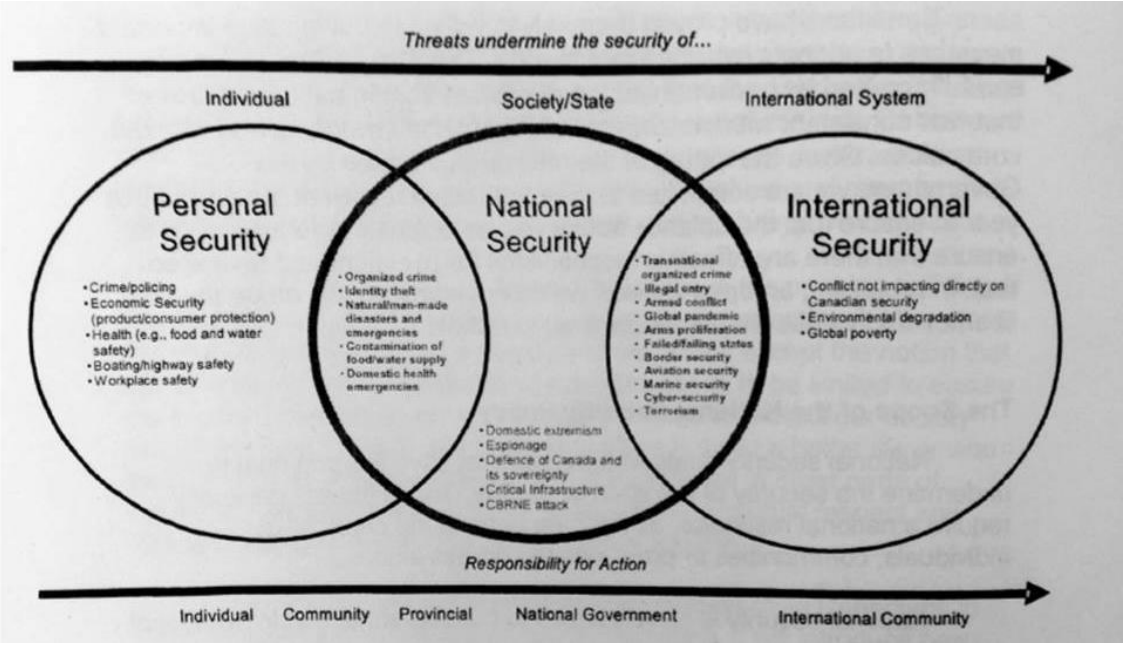

Figure 1: Venn Diagram Showing how National Security Interacts with Personal Security and International Security

Source: Alan J. Stephenson, "Canadian National Security Culture: Explaining post 9/11 Canadian National Security Policy Outcomes" (PhD thesis, Carleton University, 2016), 368.

The National Security and Intelligence Committee of Parliamentarians (NSICP) has adopted a definition of national security to help determine what it can examine.[10] The NSICP has decided that something affects national security if it:

…involve[s] at least one of the core members[11] of the security and intelligence community…and be national in character, understood as relating to threats to the

[9] Privy Council Office, *Securing an Open Society; Canada's National Security Policy*, (Ottawa: Privy Council Office, 2004), 3.

[10] National Security and Intelligence Committee of Parliamentarians, *Annual Report 2018* (Ottawa: National Security and Intelligence Committee of Parliamentarians, 2019), 13.

security of Canada as defined in the *CSIS Act*, or criminality of national scope or gravity.[12]

The *CSIS Act* includes "espionage or sabotage that is against Canada or is detrimental to the interest of Canada…" as threats to national security.[13] Therefore, the GoC's national security policy is consistent with the NSICP interpretation of national security, at least in terms of including espionage and sabotage to critical infrastructure as threats to national security.

Even with the policy and NSICP definitions of national security, there is room for interpretation. Additionally, due to the absence of a legal definition of national security, the GoC has some flexibility in determining what affects national security. Despite the ambiguity around the definition, the GoC responsibilities with respect to national security are quite clear. The preamble to the *National Security Act* states, "a fundamental responsibility of the Government of Canada is to protect Canada's national security and the safety of Canadians".[14] Therefore, it is clear that the GoC must act to protect Canada's national security, despite the potential ambiguity over what national security is.

WHY HUAWEI MIGHT BE A THREAT TO NATIONAL SECURITY

5G Technology

Understanding the evolution of cellular technology helps contextualize the impact that 5G technology will have on society. The first generation (G) of wireless technology enabled speech service, 2G enabled text and pictures to be transmitted, 3G enabled "Global

---

[11] The core members include: National Security and Intelligence Advisor, Communications Security Establishment, Canadian Security Intelligence Service, Royal Canadian Mounted Police, Department of National Defence/Canadian Armed Forces, Global Affairs Canada, Canada Border Services Agency, and Integrated Terrorism Assessment Center. See National Security and Intelligence Committee of Parliamentarians, *Annual Report 2018* (Ottawa: National Security and Intelligence Committee of Parliamentarians, 2019), 20.

[12] National Security and Intelligence Committee of Parliamentarians, *Annual Report 2018* (Ottawa: National Security and Intelligence Committee of Parliamentarians, 2019), 13.

[13] Canadian Security Intelligence Service Act, R.S.C., c. C-23, (1985).

[14] National Security Act, S.C., c. 13, (2019).

Positioning System (GPS), video conferencing, and multi-media streaming",[15] while 4G enabled the 'app economy'.[16] 5G networks are expected to be one of the most complex systems ever designed with increased speed,[17] reliability, and capacity and reduced latency over 4G systems.[18] 5G technology has the potential to enable vehicular communications,[19] autonomous vehicles,[20] individual monitoring for healthcare, robotic surgeries, improved artificial intelligence for manufacturing technologies, improved supply chain management, and efficiencies in the energy and agricultural sectors.[21]

Who Is Huawei and What Is Their Role in 5G

The implications that 5G technology will have on society are not yet fully understood, but it has the potential to change how the world operates. Huawei Technologies Co. Ltd, based in Shenzhen China, is a privately owned Chinese company,[22] and, as per Figure 2, it is one of the largest manufacturers of wireless technology in the world. According to Huawei's 2019 annual report, they "operate in more than 170 countries and regions, serving more than three billion people around the world".[23] Huawei is also one of the only companies that

---

[15] Department of Homeland Security, *Overview of Risks Introduced by 5G Adoption in the United States*, (Cybersecurity and Infrastructure Security Agency, 2019), 2.

[16] James Lewis, *How will 5G Shape Innovation and Security: A Primer,* (Center for Strategic & International Studies, Washington, 2018), 6.

[17] *Ibid.,* 6.

[18] Department of Homeland Security, *Overview of Risks Introduced by 5G Adoption in the United States*, (Cybersecurity and Infrastructure Security Agency, 2019), 2.

[19] Syed Adeel Ali Shah, Ejaz Ahmed, Muhammad Imran, and Sherali Zeadally. "5G for Vehicular Communications." *IEEE Communications Magazine* 56, no. 1 (2018): 111-117.

[20] X. Krasniqi, E Hajrizi, "Use of IoT Technology to Drive the Automotive Industry from Connected to Full autonomous Vehicles" IFAC PapersOnLine 49, Issue 29. (2016): 273, https://www.sciencedirect.com/search?qs=use%20of%20iot%20technology%20to%20drive%20the%20automotive&authors=krasniqi

[21] CB Insights, "What is 5G? understanding The Next-Gen Wireless System Set to Enable our Connected Future", last accessed 24 March 2020, https://www.cbinsights.com/research/5g-next-gen-wireless-system/

[22] Huawei, *2019 Annual Report,* (Shenzhen: Huawei, 2020), 8.

[23] Huawei, *2019 Annual Report,* (Shenzhen: Huawei, 2020), 9.

intends to produce the entire spectrum of technology required for a 5G network.[24] Huawei Technologies Canada Co., Ltd registered as a corporation in Canada on 5 March 2008,[25] and is a subsidiary of Huawei Technologies Co. Ltd.[26]

Potential National Security Concerns Regarding Huawei

The 5G technologies that Huawei will produce will potentially impact telecommunications, healthcare, manufacturing, agriculture and the energy sector just to name a few.[27] Those sectors alone represent five of the ten critical infrastructure[28] sectors identified by the GoC,[29] and according to GoC's national security policy and the NSICP disruption to critical infrastructure poses a threat to national security.[30]

---

[24] James Lewis, *How will 5G Shape Innovation and Security: A Primer,* (Center for Strategic & International Studies, Washington, 2018), 6.

[25] Government of Canada, "Federal Corporation Information", last accessed 5 April 2020, https://www.ic.gc.ca/app/scr/cc/CorporationsCanada/fdrlCrpDtls.html?lang=eng&corpId=6934986

[26] Office of the Commissioner of Lobbying of Canada, "Registry of Lobbyists", last accessed 5 April 2020, https://lobbycanada.gc.ca/app/secure/ocl/lrs/do/clntSmmry?clientOrgCorpNumber=278764&sMdKy=1370770651439

[27] CB Insights, "What is 5G? understanding The Next-Gen Wireless System Set to Enable our Connected Future", last accessed 24 March 2020, https://www.cbinsights.com/research/5g-next-gen-wireless-system/

[28] "Critical Infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective function of the government." The ten critical infrastructure sectors are: Energy and utilities, Finance, Food, Transportation, Government, Information and Communication Technology, Health, Water, Safety, and Manufacturing. See Canada, *National Strategy for Critical Infrastructure*, Ottawa, 2009, 2.

[29] Government of Canada, *National Strategy for Critical Infrastructure*, (Ottawa: 2009), 2.

[30] Privy Council Office, *Securing an Open Society; Canada's National Security Policy*, (Ottawa: Privy Council Office, 2004), 4.

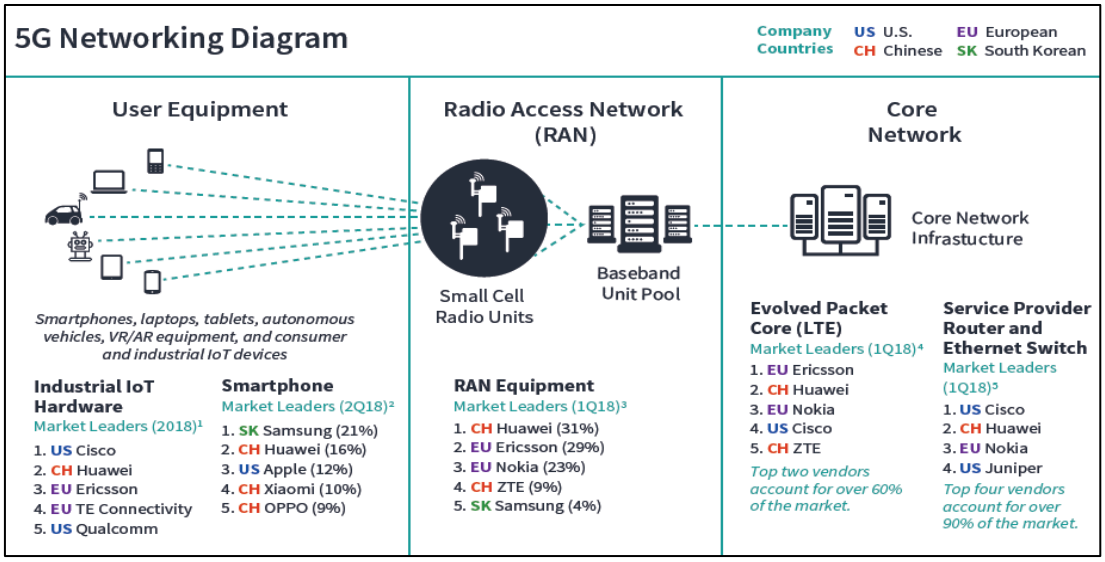

Figure 2: 5G Networking Diagram and Current 4G LTE Equipment Manufacturing

Source: James, Lewis, *How will 5G Shape Innovation and Security: A Primer,* (Center for Strategic & International Studies, Washington, 2018), 4.

One of the national security concerns around 5G's use in critical infrastructure originates from the fact that vendors could potentially put 'backdoors' in the technology allowing the interception of calls and information, or potentially sabotaging the network.[31] A 'backdoor' could be put into the equipment during manufacturing, or through a support arrangement where an upgrade or patch for the system is introduced, thereby changing how that system operates.[32]

As per Figure 2, none of the major telecom equipment manufacturers are Canadian companies, therefore the same threat exists regardless of which manufacturer is used. However, unique from other 5G manufacturers,[33] Huawei has been publically identified as

[31] Tom Uren, "The technical reasons why Huawei is too great a 5G risk", *Huawei and Australia 5G Network*, (Australian Strategic Policy Institute, 2018), 8.

[32] Olav Lysne, The Huawei and Snowden Questions: *Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?* (Cham: Springer Open, 2018), 5.

[33] Nokia, for example, a Finish company has been provided $40 millions dollars by the GoC to conduct research for Canada's 5G network. See, CBC News, "Ottawa Pledges $40M for Nokia to

potentially a risk to national security.[34] Canada's lack of trust in Huawei may be due to ties that Huawei's founder, Ren Zhengfei, is alleged to have with the People's Liberation Army (PLA) and the Communist Party of China (CPC). Zhengfei acknowledged his employment at a synthetic fabric factory while serving in the military, and that he subsequently joined the CPC, but indicates that those relations have no impact on Huawei operations.[35]

Others, however, have claimed that Zhengfei actually worked for the military department responsible for telecom research and that Huawei has a relationship with the Chinese military.[36] The concern is, therefore, that Huawei is potentially working for the Chinese Government and may also take direction from the CPC. In 2012, the United States (US) House of Representatives Permanent Select Committee on Intelligence (HRPSCI) investigated the claim that the Chinese Government was able to exert "influence or control over the Chinese telecommunications companies".[37] Huawei claimed that the company is privately owned and not influenced by the Chinese Government or the CPC.[38] Huawei did, however, indicate that the shareholder agreement gives veto power to Ren Zhengfei,[39] and that the CPC Committee exists within Huawei, as required by Chinese law, but did not clarify how Huawei and the Committee interact.[40]

---

conduct 5G research", last accessed 13 April 2020, https://www.cbc.ca/news/business/government-nokia-huawei-5g-1.4991435

[34] CBC News, "New public safety minister says Huawei 5G review 'a priority' but offers no timeline" last accessed 25 April 2020, https://www.cbc.ca/news/politics/5g-huawei-china-bill-blair-1.5367002

[35] Reporter, SCMP. "Transcript: Huawei Founder Ren Zhengfei's Responses to Media Questions at a Round Table this Week." South China Morning Post Publishers Limited, last modified Jan 16.

[36] Evan S. Medeiros, Roger Cliff, Keith Crane, and James C. Mulvenon, *A New Direction for China's Defense Industry*. (Santa Monica, CA: RAND Corporation, 2005) 218.

[37] United States, Congress House Select Committee on Intelligence. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. (Congressional Publications, 2012), 13.

[38] *Ibid.,* 14.

[39] *Ibid.,* 14.

[40] *Ibid.,*23.

Although the HRPSCI did not prove any relation between Huawei and the Chinese Government or the CPC, the HRPSCI concluded that Huawei "likely remains dependent on the Chinese government for support".[41] The report also concluded that the "evidence undermines [Huawei's] claim of [its US operations] being a completely independent subsidiary of Huawei's parent company in Shenzhen, China."[42] More recently, in May 2019, the US government added Huawei to its Entity List, indicating that the company is a national security threat and preventing US companies from doing business with them.[43]

Even if there are no formal connections between Huawei and the Chinese Government, or the CPC, Chinese law is also grounds for Canadian concern. The *National Intelligence Law of the P.R.C. (2017)* provides the Chinese National Intelligence Work Institutions with significant authority.[44] Article 7 [45] and Article 14 [46] of the act require Huawei, by law, to assist the Chinese intelligence institutions if requested to do so. In theory, this assistance could include putting 'backdoors' in 5G technology so that the Chinese could intercept information from the network (i.e. espionage) or sabotage critical infrastructure. Although required by law, Zhengfei has indicated that Huawei would say no to any request

[41] *Ibid.*,13.

[42] *Ibid.*,29.

[43] Department of Public Safety, "Fifth Generation Wireless Technology (5G)", last accessed 25 April 2020, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/031/index-en.aspx

[44] China Law Translate. "National Intelligence Law of the P.R.R. (2017)" last accessed 11 April 2020, https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

[45] Article 7 states "All organizations and citizen shall support, assist and cooperate with national intelligence efforts in accordance with the law…" See, China Law Translate. "National Intelligence Law of the P.R.R. (2017)" last accessed 11 April 2020, https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

[46] Article 14 of the law states: "National intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation" See, China Law Translate. "National Intelligence Law of the P.R.R. (2017)" last accessed 11 April 2020, https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

from the government to access its customers' data and that he would rather shut the company down than "damage the interest of their customers".[47]

Despite the suspicions around Huawei's relationship with the Chinese Government and the CPC, and the concerns around Chinese law, there is no proof, at least in the public domain, of Huawei conducting, or supporting, espionage or sabotage. In fact, Huawei was part of the security review program carried out on the Canadian 3G/4G telecommunications network,[48] and Huawei has components in those networks.[49]

Since then, however, it would appear that Canada has increasing concerns about Chinese cyber attacks. In 2014, the Communications Security Establishment (CSE) Canada discovered that a "highly sophisticated Chinese state-sponsored actor" had hacked Canada's National Research Council's computer system.[50] In 2018, Canada, along with the other Five Eyes nations,[51] indicated that multiple cyber attacks had occurred and that CSE Canada assessed "that it is almost certain that actors likely associated with the Peoples' Republic of China (PRC) Ministry of State Security are responsible for the compromise…beginning as early as 2016."[52] These public accusations by the GoC against the Chinese Government may

---

[47] China Law Translate. "National Intelligence Law of the P.R.R. (2017)" last accessed 11 April 2020, https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

[48] Canadian Centre for Cyber Security. "CSE's Security Review Program for 3G/4G/LTE in Canadian Telecommunications Networks" last accessed 23 March 2020, https://cyber.gc.ca/en/news/cses-security-review-program-3g4glte-canadian-telecommunications-networks

[49] CBC, "Northern Canada Could be left out in the cold if Ottawa passes Huawei 5G ban", last accessed 26 April 2020, https://www.cbc.ca/news/canada/north/opinion-huawei-northern-telecom-1.5479193

[50] Canadian Broadcasting Corporation. "Chinese cyberattack hits Canada's National Research Council", last accessed 16 April 2020, https://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241

[51] Security Week. " 'Five Eyes' Nations Blame China for APT10 Attacks" last accessed 16 April 2020, https://www.securityweek.com/five-eyes-nations-blame-china-apt10-attacks

[52] Communications Security Establishment. "Canada and Allies Identify China as Responsible for Cyber-Compromise" last access 16 April 2020, https://cse-cst.gc.ca/en/media/media-2018-12-20

signify a lack of trust in China, and a suspicion that Huawei may be used to gain access to Canada's 5G network; thereby, posing a threat to Canada's national security.

SOLUTION SPACE – FIVE EYES INTELLIGENCE COMMUNITY

As the GoC decides what to do with respect to Huawei's access to Canada's 5G network, it is undoubtedly looking at like-minded states, particularly the Five Eyes[53] members, to assess what actions they have taken. Canada is the only Five Eyes member that has not made a decision with respect to Huawei. As previously discussed, the US has added Huawei to its Entity List thereby banning the use of its components,[54] and Australia has also banned Huawei from accessing their 5G network.[55] The United Kingdom (UK) has restricted Huawei's access to components of the 5G network that do not affect security critical networks and functions.[56] Additionally, the UK has imposed a cap on the percentage of Huawei equipment that can be used on the network.[57] New Zealand intends to reviews proposals, including those that propose to use Huawei technology, from telecommunications providers on a case-by-case basis to assess the national security risk before making a decision.[58]

The decisions made by Canada's closest intelligence partners have all in some way restricted or fully denied Huawei's access to their 5G networks. This potentially indicates that they believe Huawei poses a potential threat to their national security. The decisions made by

---

[53] The Five Eyes intelligence community is the "most exclusive intelligence sharing club in the world"[53] and Canada gains considerable intelligence from being part of this group. See, James Cox, *Canada and the Five Eyes Intelligence Community* (Canadian Defence & Foreign Affairs Institute and Canadian International Council, 2012), 4.

[54] Department of Public Safety, "Fifth Generation Wireless Technology (5G)", last accessed 25 April 2020, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/031/index-en.aspx

[55] *Ibid.*

[56] UK Foreign Secretary, "Foreign Secretary's statement on Huawei", last accessed 25 April 2020, https://www.gov.uk/government/speeches/foreign-secretary-statement-on-huawei

[57] *Ibid.*

[58] Department of Public Safety, "Fifth Generation Wireless Technology (5G)", last accessed 25 April 2020, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/031/index-en.aspx

the Five Eyes partners indicates the solution space that Canada has for making a decision. Canada could decide to allow unrestricted access to its 5G network, albeit none of the Five Eyes partners have, it could restrict the scope and scale of Huawei's access, or it could completely deny access to the network. The existing Canadian statutes, treaty provisions and policy tools that are at the GoC's disposal to enable or constrain that decision will be explored in the following sections.

STATUTES AND TREATY PROVISIONS

A statute is "a law passed by the legislative branch of a government".[59] The GoC must abide by any Canadian statutes; therefore justifying a decision, with respect to Huawei's access to Canada's 5G network, based on existing Canadian statutes will provide credibility to that decision. A treaty is "an international agreement concluded between States in written form and governed by international law…"[60] Although, it is in the GoC's interest to adhere to international law, in the case of allowing Huawei access to Canada's 5G network, if the GoC's decision appeared to contradict international law, the GoC could still make the decision but may face political or economic consequences.[61]

Foreign Investment - *Investment Canada Act*

The *Investment Canada Act* (*ICA*) allows the GoC to review significant investments in Canada by non-Canadians to ensure that those investments are in the economic interest of Canada.[62] Additionally, the *ICA* allows for the review of any investments in Canada by a non-

[59] Department of Justice, "Definition", last accessed 24 April 2020, https://www.justice.gc.ca/eng/csj-sjc/ccs-ajc/06.html

[60] United Nations, *Vienna Convention on the Law of Treaties 1969*, volume 1155, (Vienna, 1980), 333.

[61] Conversation with Dr. E. Kirley, Professor of Technology and Law at the University of Osgood Hall Law School, and Matthew Maxwell 13 April 2020.

[62] National Security Act, S.C., c. 13, (2019).

Canadian if it could be injurious to national security,[63] although the Act, itself, doesn't define national security. The Minister of Innovation, Science and Economic Development (ISED) is responsible for the administration of the *ICA,* and consults with the Minister of Public Safety and Emergency Preparedness "for referring investments that could be injurious to national security to the Governor in Council (GiC), who may order a review".[64] The review process is supported by Public Safety and the investigative bodies as defined in the National Security Review of Investments Regulations.[65] Once the review is completed, it is referred to the GiC for a decision to allow the investment, with or without conditions, disallow the investment or "divest control of the Canadian business or its investment in an entity".[66] The guidelines for conducting a national security review provide a list of some potential factors that the GiC may take into consideration when making a determination. Three factors from this list that may be applicable to Huawei's investment in Canada's 5G network are:[67]

- If the investment might affect critical infrastructure;
- If the investment might enable foreign surveillance or espionage; and
- If the investment might impact Canada's international interest, including foreign relationships.

The guideline that enables the government to assess the impact on Canada's international interest, including foreign relationships, may be of particular importance. The US Government has warned Canada that if they allow Huawei access to their 5G network, that the US would stop providing Canada access to US intelligence.[68] If the US followed

---

[63] *Ibid.*

[64] Government of Canada. "Guidelines on the National Security Review on Investments", last access 16 April 2020, https://www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html

[65] *Ibid.,*

[66] *Ibid.*

[67] *Ibid.*

[68] Fife, Robert and Chase, Steven. "Top White House Official Lays Out U.S. Case for Banning Huawei from Canada's 5G Network: U.S. Official Robert Blair Met with Public Safety Minister Bill Blair and Senior Officials from the CSIS, CSE and the Departments of Innovation and Foreign Affairs." The Globe and Mail, last modified Mar 09.

through on this threat, there would be a significant impact on Canada's intelligence capabilities, and it would likely result in Canada being banned from the Five Eyes, although to date the UK and New Zealand are still members despite not banning Huawei in their 5G networks.

According to a 2019 briefing note for the Minister of Public Safety on 5G technology, a working group had been established with members from "Public Safety, CSE, Global Affairs Canada, National Defence, Innovation, Science, and Economic Development, the Canadian Security Intelligence Service, and the Privy Council Office" to assess the "economic opportunities and security risks associated with 5G technology".[69] Although the working group appears to focus on 5G technology at large, and not specifically Huawei, based on the described scope of the working groups review, it fits the criteria of a national security review that would be carried out under the *ICA.* An email from Public Safety Canada did not confirm or deny if the examination was being carried out under the *ICA*, only indicating it's "being conducted as part of Public Safety Canada's mandate of exercising federal leadership and ensuring national level coordination across all federal departments and agencies responsible for national security...".[70] The email from Public Safety Canada also said that "the examination is congruent with the objectives of Canada's National Cyber Security Strategy",[71] however, due to when the response was received, there was insufficient time to determine the relevance of the strategy to this paper. In general, receiving a concrete response from the GoC, through their websites, to specific questions was challenging. This may be due

[69] Government of Canada. " Fifth Generation Wireless Technology (5G)", last accessed 1 April 2020, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/031/index-en.aspx

[70] Email General Enquiries Public Safety Canada to Major Maxwell, Public Enquiry - Security Risk associated with 5G Technology BN, received 28 April 2020.

[71] *Ibid.*

to the complexity of the issue, and the fact that the issue spans several federal departments, but this reality, in addition to the fact that decisions by the GoC on this issue are Cabinet Confidential, made it challenging to find primary sources on the subject of allowing, or denying, Huawei access to Canada's 5G network.

A review carried out under the *ICA* would enable the GoC to determine the scope of the potential threat, and hence what options are available to mitigate or eliminate the threat. The fact that the *ICA* does not define national security provides the GoC some flexibility in their interpretation and decision making.

Depending on the results of the review, the *ICA* would allow the GoC to restrict Huawei Technologies Canada Co., Ltd from selling any 5G components in Canada. Alternatively, they could restrict them from selling certain 5G components in Canada. A benefit of the *ICA* is that any decision made with respect to Huawei would not affect any of the other suppliers of 5G technology.

Trade Agreements

The *ICA* is a tool that the GoC could potentially use to prevent Huawei Technologies Canada Co., Ltd., from investing in 5G technology and therefore selling it to Canadian telecom companies. The *ICA* would not, however, prevent Canadian telecom companies from importing Huawei equipment for their 5G networks.

Canada and China are both members of the World Trade Organization (WTO),[72] so Huawei Technologies Co. Ltd., the parent company to Huawei Technologies Canada Co., Ltd., could sell 5G technology to Canadian telecom companies. Canada could, however,

[72] World Trade Organization, "Members and Observers", last accessed 1 May 2020, https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm

invoke the national security exemption, Article XXI, in the General Agreement on Tariffs and Trade (GATT) banning its import. Article XXI of the GATT states that:

> "nothing in the agreement shall be construed to…prevent any contracting party from taking any action which is considers necessary for the protection of its essential security interest…taken in time of war or other emergency in international relations."[73]

Craig Forcese[74] has indicated that "the term 'essential security interest' is not a legal term of art. It is, therefore, fraught with ambiguity. Indeed, this exception has proven elastic in the past."[75] Although he also indicates that there are doubts that a WTO panel would question a state's use of the exemption,[76] countries have been accused of using it "as a pretext for protectionist policies".[77]

Due to the potential issues surrounding the GATT, other statutes should be considered. The *Export and Imports Permits Act*, allows the Minister Global Affairs Canada to exercise "wide discretionary powers to control the flow of goods contained in the specified lists provided in the Act" .[78] However, according to Forcese, it is unlikely that the *Export and Import Permits Act* is a tool that could be used to prevent the import of Huawei components.[79]

---

[73] World Trade Organization, "The General Agreement on Tariffs and Trade", (Geneva: 1986), 38-39

[74] Craig Forcese was appointed to the National Security and Intelligence Review Agency by the Prime Minister in 2019 (see, PM, Prime Minister announces members of the new National Security and Intelligence Review Agency, last accessed 2 May 2020, https://pm.gc.ca/en/news/news-releases/2019/07/24/prime-minister-announces-members-new-national-security-and) and he is a Full Professor in the Faculty of Law at the University of Ottawa.

[75] Craig Forcese and West, *National Security Law 2nd Edition – Chapter 6*, Unpublished, 14.

[76] *Ibid.*,15.

[77] *Ibid.*,14 - 15.

[78] Government of Canada, Import and Export Controls – Importing", last accessed 20 April 2020, https://www.international.gc.ca/controls-controles/about-a_propos/impor/importing-importation.aspx?lang=eng.

[79] Craig Forcese and West, *National Security Law 2nd Edition - Chapter 6*, Unpublished, 17

This is likely due to the items that the import controls list (ICL) includes, which are: textiles and clothing, agricultural products, steel products, aluminum products, and firearms.[80]

Precedence

In May 2012 the GoC invoked the national security exemption (NSE) "for all procurements of goods and services related to email, networks, and data centre infrastructure..." for the GoC network.[81] In 2012, the invocation of the NSE was applicable to GoC procurements only, and therefore did not affect Canadian telecom companies. The NSE can be applied by the GoC under any of its existing trade agreements when it conducts any procurement.[82] In 2012, after confirming that the NSE had been invoked for the building of the GoC's computer network, the Prime Minister's director of communications eluded to the fact that the NSE could have been invoked, at least partially, to deny Huawei from being able to bid on the network.[83] Due to the fact that the GoC's decision to invoke the NSE was Cabinet Confidential, and any information that went into that decision would have been classified it is difficult to determine what the GoC would have done if Huawei had made a bid.

Although ambiguous, Article XXI of the GATT would allow Canada to prevent Huawei from importing some, or all, of their 5G technology to Canada. China may challenge Canada's decision through the WTO, but it's unlikely that the WTO would question Canada's

---

[80] Government of Canada, Import and Export Controls – About Us", last accessed 20 April 2020, https://www.international.gc.ca/controls-controles/about-a_propos/index.aspx?lang=eng.

[81] House of Commons. Standing Committee on Government Operations and Estimates. *Evidence*, 23 February 2017.

[82] Government of Canada Supply Manual, National Security Exception, last accessed 26 March 2020, https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/3/105

[83] The Globe and Mail, "Ottawa set to ban Chinese Firm from Telecommunications Bid' last accessed 20 April 2020, https://www.theglobeandmail.com/news/politics/ottawa-set-to-ban-chinese-firm-from-telecommunications-bid/article4600199/

decision.[84] Finally, using Article XXI of the GATT would only apply to Huawei so the decision would not impact the ability of Canadian telecom companies to import from other manufacturers of 5G technology.

Telecommunications Act

Due to the ambiguity of Article XXI of the GATT, Forcese suggests that from a trade perspective other "regulatory action would [likely] be needed to block the use of problematic technologies in Canadian critical infrastructure".[85] He suggests that there are sections of the *Telecommunications Act* which may support this.[86] Section 15 of the Act allows the minister to "establish standards in respect of the technical aspects of telecommunications…"[87] Part IV.1 of the Act allows the Minister to establish requirements for the registration of any telecommunication equipment, and if that equipment is not registered it cannot be sold, imported, distributed or leased in Canada.[88]

If the GoC created a standard for 5G technology, or 5G networks, that mitigated the risks associated with using Huawei's 5G technology, they could make the standard a prerequisite for registration. If the prerequisite standard for registration was not met, the equipment could not be imported, sold, leased or distributed in Canada, thereby achieving the aim.

The practicalities of defining standards and/or registration requirements that would mitigate Huawei's ability to spy or sabotage Canada's 5G network are beyond the scope of this paper. This option, however, does potentially provide the GoC some regulatory options to deal with technologies that may pose a threat to Canada's national security.

---

[84] Craig Forcese and West, *National Security Law 2nd Edition – Chapter 6*, Unpublished, 15.
[85] *Ibid.*, 17.
[86] *Ibid.*, 17.
[87] Telecommunications Act, S.C., c. 38, s. 15 (1993).
[88] *Ibid.*

The option of creating a standard could potentially mitigate the threat posed by Huawei's 5G technology, but the same standards would also apply to all other 5G technology manufactures. If the standard is too difficult to meet, or does not effectively mitigate the risk of espionage or sabotage, it may not be an effective or useful approach. Additionally, if the standard is different from the rest of the world, it may become impractical or may be excessively expensive.

Emergency Management Act

The statutes and treaty provisions provide the GoC options with respect to preventing Huawei from selling their 5G technology to Canadian telecom companies. The *Emergency Management Act (EMA)* deals with how the GoC is supposed to plan for emergencies, including those that could affect national security. According to the *EMA*, all ministers are to identify risks within their area of responsibility and develop emergency management plans (EMP) for those risks "in accordance with the policies, programs and other measures established by the Minister [of Public Safety]".[89]

If the GoC assessed that Huawei's access to its 5G network posed a threat to Canada's national security, the *EMA w*ould require that the GoC develop an emergency management plan to address that risk. That plan would be developed based on the policies and programs established by the Minister of Public Safety, therefore, the current policies and programs that Canada has in place must be reviewed to assess how it may enable or constrain the GoC decision.

[89] Emergency Management Act, S.C., c. 15 (2007).

CANADIAN POLICIES THAT ENABLE OR CONSTRAIN A DECISION

For the purpose of this paper, government policy should be interpreted as a statement of what the government intends to do. Since policy is not law, the government can decide whether or not the policy is followed.

Canada's policy objective for Emergency Management is to "promote an integrated and resilient whole-of-government approach to emergency management planning, which includes better prevention/mitigation[90] of, preparedness for, response to, and recovery from emergencies."[91] The policy highlights the complexity of threats to Canada's national security, specifically mentioning the interdependence of critical infrastructure and attacks on networks.[92] Under the policy requirements, in accordance with the *EMA*, ministers are to identify risks[93], including those related to critical infrastructure, and develop EMPs based on those risks.[94] The EMP should include how to mitigate/prevent, prepare for, respond to, and recover from hazards[95] that introduce risk.[96]

If the GoC assessed that it could not adequately prepare for, respond to, or recover from the threat of Huawei using its access to the 5G network for espionage or sabotage, then the GoC would have to mitigate/prevent the risk. It may be determined that the only way to effectively mitigate/prevent the potential threat posed by Huawei would be to deny their access to the network. Alternatively, if the GoC assessed that they could prepare for, respond

---

[90] Prevention/mitigation is actions taken in order to adapt to, eliminate or reduce the impact of disasters in order to protect lives, property, the environment, and reduce economic disruption. See, Public Safety Canada, *An Emergency Management Framework for Canada 3rd Edition*, 2017, 22.

[91] Government of Canada, Federal Policy for Emergency Management – Building a Safe and Resilient Canada, (Ottawa: Public Safety Canada, 2012), 1.

[92] *Ibid.*,1.

[93]Risk is the combination of the likelihood and the consequence of a specified hazard being realized. See, Canada. *Federal Policy for Emergency Management – Building a Safe and Resilient Canada*. Ottawa: Public Safety Canada, 2012.

[94] *Ibid.*,3.

[95] A hazard is a potentially damaging physical event, phenomenon or human activity that may cause the loss of life or injury, property damage, social and economic disruption or environmental degradation. See, Public Safety Canada, *An Emergency Management Framework for Canada 3rd Edition*, 2017, 7.

[96] *Ibid.*,3.

to, or recover from the potential treat posed by Huawei, then they may be able to put measures in place that would make Huawei's access to the network acceptable from a national security perspective.

POTENTIAL DECISION SPACE

The GoC has several options when it comes to making a decision on whether or not to allow Huawei access to Canada's 5G network, all of which are enabled or constrained by existing statutes, treaty provisions and policies. The GoC can decide to allow Huawei unrestricted access to the network, it can allow restricted access to the network, or it can deny access to the network. The decision will be based on the perceived threat posed by Huawei in addition to the GoC's capability to mitigate or eliminate the threat. The threat and the GoC's ability to deal with that threat should be well understood by conducting a national security review under the authority of *ICA*. With this information the GoC can formulate a decision using the framework in the Policy for Emergency Management.

Allow Full Unrestricted Access

If the GoC assesses that it can properly prepare for, respond to, and recover from any activities that Huawei may take on Canada's 5G network without restricting trade, investment, or by taking regulatory action they could allow Huawei full and unrestricted access. This decision would be supported by the GoC's policy on emergency preparedness and there would be no requirement to rely on any Canadian statutes or treaty provisions discussed in this paper.

Allow Access with Restrictions

If the GoC does not believe that it is able to properly prepare for, respond to, and recover from any activities that Huawei may take if they have unrestricted access to Canada's

5G network they may be able to mitigate that risk to an acceptable level by restricting Huawei's access. There are several statutes and treaty provisions which Canada can use to mitigate the potential risks. The *ICA* and Article XXI of the GATT would allow the GoC to restrict Huawei from selling and importing specific components, thereby limiting what portions of the network Huawei would have access to. Similar to the UK, it may be possible to restrict Huawei's access to security critical networks and functions, thereby reducing the risks to Canada's critical infrastructure.

In addition to, or independent from, the trade and investment restrictions, under the *Telecommunications Act*, the GoC could impose standards on some, or all, of the 5G components if it believes that those standards will reduce Huawei's ability to spy on Canadians or sabotage critical infrastructure. Again, acting under the *Telecommunications Act*, the GoC could make registration of some, or all, of the 5G components dependent on meeting that standard. Without that registration the components could not be imported, leased, distributed or sold in Canada.[97] These standards, however, would not apply only to Huawei but to all 5G component manufacturers even if they are not perceived to pose a threat to national security.

The GoC could also, as it did in 2012, only restrict Huawei from having access to the GoC's network, and not put any restrictions on publicly used equipment. Although this is possible, given the large amount of critical infrastructure that is publically owned, 85% is not owned or operated by the federal government,[98] this likely does very little to protect the majority of Canada's critical infrastructure.

---

[97] Telecommunications Act, S.C., c. 38, s. 69 (1993).

[98] Andrew Graham, *Canada's Critical Infrastructure – when is Safe Enough Safe Enough?*, (Macdonald-Laurier Institute for Public Policy, 2011), 23

Restrict Huawei Completely from the 5G Network

If the GoC assesses that it cannot properly prepare for, respond to and recover from activities that Huawei may take, even with the mitigations measures discussed in the preceding section, they could prevent the threat, and ban Huawei from accessing the 5G network. This could be accomplished using the *ICA* and Article XXI of the GATT to prevent the sale and import of any Huawei 5G components in Canada.

CONCLUSION

The national security review will advise the GoC on the potential national security risks of allowing Huawei access to its 5G network. Based on those risks, the GoC should be able to determine whether they can allow Huawei unrestricted access to the network, allow them restricted access to the network, or deny them any access to the network.

Whatever that decision is, it can be supported with existing Canadian statutes, treaty provisions and GoC policy. The *ICA* will enable the GoC to restrict or deny Huawei's investment of 5G in Canada. Although the wording of Article XXI of the GATT is considered by some legal scholars to be ambiguous, if the GoC decides to use it to prevent the importation of any, or all, of Huawei's 5G technology, it is unlikely the WTO would question that decision and even if they did the GoC could still decide to ban importations. Finally, the *Telecommunications Act* provides the GoC options with respect to imposing technical standard on 5G technology, to mitigate/eliminate the risk of espionage and sabotage by Huawei, but it will have the potentially negative effect of making those standards applicable to all 5G technology manufacturers. The application of those statutes and treaty provisions can be explained under the framework of Canada's Policy of Emergency Management, which originates from the *Emergency Management Act*. Additionally, unless the GoC decides to allow Huawei unrestricted access to its 5G network, any decision, enabled by the statutes,

treaty provisions and GoC policy, to restrict access or deny access to the network would be consistent with its Five Eyes intelligence community partners.

The decision to allow, deny, or restrict Huawei's access to the 5G network is, however, not likely to be made solely on the threat to national security. The GoC will have to consider the economic and political implications of any decision. If they decide to deny or severely restrict Huawei's access to the network, the political relationships with China may become more strained. If Huawei is allowed access to the network, even if restricted, the US may follow through on its threat to deny Canada intelligence that is currently shared. Domestically there may be implications if Canadians believe that the GoC is allowing the Chinese to spy on them, or, alternatively, the restriction or denial of Huawei may cause an increase in price for 5G services which may upset some of the domestic population.

Although the focus of this paper has been on the statutes, treaty provisions, and policy instruments that would enable or constrain the GoC decision to allow, or deny, Huawei's access to its 5G network, the actual decision space will be much more complicated once the economic and political considerations are taken into account. Though the decision space is more complicated, the decision is still to either allow Huawei unrestricted access to the network, allow it restricted access to the network, or deny its access to the network. While the details of the decision making process will not be made public, as it will be Cabinet Confidential, the statutes, treaty provisions and policies discussed in this paper may enable that decision.

BIBLIOGRAPHY

Canada. House of Commons. Standing Committee on Government Operations and Estimates. *Evidence*, 23 February 2017.

Canada. National Security and Intelligence Committee of Parliamentarians. *Annual Report*. Ottawa: National Security and Intelligence Committee of Parliamentarians, 2019.

Canada. Privy Council Office. *Securing an Open Society: Canada's National Security Policy*. Ottawa: Privy Council Office, 2004.

Canada. Innovation, Science and Economic Development Canada, *Investment Canada Act – Annual Report 2018 – 2019*, Ottawa: Innovation, Science and Economic Development Canada, 2019.

Canada. *Federal Policy for Emergency Management – Building a Safe and Resilient Canada*. Ottawa: Public Safety Canada, 2012.

Canada, *National Strategy for Critical Infrastructure*, Ottawa, 2009.

Canada, "Federal Corporation Information", last accessed 5 April 2020, https://www.ic.gc.ca/app/scr/cc/CorporationsCanada/fdrlCrpDtls.html?lang=eng&corpId=6934986

Canada. "Guidelines on the National Security Review on Investments", last access 16 April 2020, https://www.ic.gc.ca/eic/site/ica-lic.nsf/eng/lk81190.html

Canada, Import and Export Controls – Importing", last accessed 20 April 2020, https://www.international.gc.ca/controls-controles/about-a_propos/impor/importing-importation.aspx?lang=eng.

Canada, Import and Export Controls – About Us", last accessed 20 April 2020, https://www.international.gc.ca/controls-controles/about-a_propos/index.aspx?lang=eng.

Canada Supply Manual, National Security Exception, last accessed 26 March 2020, https://buyandsell.gc.ca/policy-and-guidelines/supply-manual/section/3/105

Canadian Centre for Cyber Security. "CSE's Security Review Program for 3G/4G/LTE in Canadian Telecommunications Networks" last accessed 23 March 2020, https://cyber.gc.ca/en/news/cses-security-review-program-3g4glte-canadian-telecommunications-networks

CBC, “Ottawa Pledges $40M for Nokia to conduct 5G research”, last accessed 13 April 2020, https://www.cbc.ca/news/business/government-nokia-huawei-5g-1.4991435

CBC, “New public safety minister says Huawei 5G review 'a priority' but offers no timeline” last accessed 25 April 2020, https://www.cbc.ca/news/politics/5g-huawei-china-bill-blair-1.5367002

CBC, “Northern Canada Could be left out in the cold if Ottawa passes Huawei 5G ban”, last accessed 26 April 2020, https://www.cbc.ca/news/canada/north/opinion-huawei-northern-telecom-1.5479193

CBC, “Chinese cyberattack hits Canada’s National Research Council”, last accessed 16 April 2020, https://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241

CB Insights. “What is 5G? understanding The Next-Gen Wireless System Set to Enable our Connected Future.” Last accessed 24 March 2020. https://www.cbinsights.com/research/5g-next-gen-wireless-system/

China Law Translate. “National Intelligence Law of the P.R.R. (2017)” last accessed 11 April 2020, https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

Communications Security Establishment. “Canada and Allies Identify China as Responsible for Cyber-Compromise” last access 16 April 2020, https://cse-cst.gc.ca/en/media/media-2018-12-20

Cox, James., *Canada and the Fives Eyes Intelligence Community*. Canadian Defence & Foreign Affairs Institute and International Council, 2012.

Department of Justice, “Definition”, last accessed 24 April 2020, https://www.justice.gc.ca/eng/csj-sjc/ccs-ajc/06.html

Dobson, Wendy. *Living with China: A Middle Power Finds Its Way*, Toronto: University of Toronto Press, 2019.

Fife, Robert and Chase, Steven. "Top White House Official Lays Out U.S. Case for Banning Huawei from Canada's 5G Network: U.S. Official Robert Blair Met with Public Safety Minister Bill Blair and Senior Officials from the CSIS, CSE and the Departments of Innovation and Foreign Affairs." The Globe and Mail, last modified Mar 09.

Forcese, Craig. *National Security Law: Canadian Practice in International Perspective*. Toronto: Irwin Law Inc. 2008.

Forcese, Craig and West, Leah., *National Security Law 2nd Edition – Chapter 6*, Unpublished.

Forbes, China is Closing the Gap with the U.S. in R&D Expenditure, last accessed 27 April 2020, https://www.forbes.com/sites/niallmccarthy/2020/01/20/china-is-closing-the-gap-with-the-us-in-rd-expenditure-infographic/#1b51b1135832

Graham, Andrew. *Canada's Critical Infrastructure: When is Safe Enough Safe Enough*?, Macdonald-Laurier Institute for Public Policy, 2011.

Huawei Cyber Security Evaluation Center Oversight Board, *Annual Report 2018*, 2018.

Huawei, *2019 Annual Report*, Shenzhen: Huawei, 2020.

Innovation, Science, and Economic Development Canada., Email Exchange between ISED and Matthew Maxwell, April 2020.

Kirley, E., Zoom Conversation between Dr. Kirley, Professor of Technology and Law at the University of Osgood Hall Law School, and Matthew Maxwell, 13 April 2020.

Krasniqi, X., Hajrizi, E., "Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles", IFAC-PapersOnLine, Issue 29 (2016): 269-274. https://www.sciencedirect.com/search?qs=use%20of%20iot%20technology%20to%20drive%20the%20automotive&authors=krasniqi

Lewis, J., *How will 5G Shape Innovations and Security: A Primer*, Washington: Center for Strategic & International Studies, 2018.

Lysne, Olav. *The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust into Electronic Equipment?*. Cham: Springer Open, 2018.

Medeiros, Evan S., Roger Cliff, Keith Crane, and James C. Mulvenon, *A New Direction for China's Defense Industry*. Santa Monica, CA: RAND Corporation, 2005.

Mills, Marcia., Email discussion between Marcia Mills, Counsel at Fasken, and Matthew Maxwell, April 2020,

Mills, Marcia., *Because We Said So: Invoking the National Security Exception to Reduce Access to Dispute Processes for Government Suppliers*, Canadian Global Affairs Institute, 2019.

New York Times, "Trump Officials Battle Over Plan to Keep Technology Out of Chinese Hands", last accessed 27 April 2020,

https://www.nytimes.com/2019/10/23/business/trump-technology-china-trade.html

Office of the Commissioner of Lobbying of Canada, “Registry of Lobbyists”, last accessed 5 April 2020, https://lobbycanada.gc.ca/app/secure/ocl/lrs/do/clntSmmry?clientOrgCorpNumber=278764&sMdKy=1370770651439

Public Safety Canada, *An Emergency Management Framework for Canada 3rd Edition*, 2017.

Public Safety Canada, Email General Enquiries Public Safety Canada to Major Maxwell, Public Enquiry - Security Risk associated with 5G Technology BN, received 28 April 2020.

Public Safety Canada, “Fifth Generation Wireless Technology (5G)”, last accessed 1 April 2020, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20191120/031/index-en.aspx

Saunders, Phillip C. “China’s Global Activism: Strategy, Drivers and Tools.” *Institute for National Strategic Studies,* Occasional Paper 4 (October 2016).

Security Week. “ ‘Five Eyes’ Nations Blame China for APT10 Attacks” last accessed 16 April 2020, https://www.securityweek.com/five-eyes-nations-blame-china-apt10-attacks

SCMP. "Transcript: Huawei Founder Ren Zhengfei's Responses to Media Questions at a Round Table this Week." South China Morning Post Publishers Limited, last modified Jan 16.

Shah, Syed Adeel Ali, Ejaz Ahmed, Muhammad Imran, and Sherali Zeadally. "5G for Vehicular Communications." IEEE Communications Magazine 56, no. 1, 2018.Stephenson, Allan J. “Canadian National Security Culture: Explaining post 9/11 Canadian National Security Policy Outcomes”, PhD thesis, Carleton University, 2016.

The Globe and Mail, “Ottawa set to ban Chinese Firm from Telecommunications Bid’ last accessed 20 April 2020, https://www.theglobeandmail.com/news/politics/ottawa-set-to-ban-chinese-firm-from-telecommunications-bid/article4600199/

Trudeau, Justin. *Minister of Public Safety and Emergency Preparedness Mandate Letter*, 13 December 2019.

United States, Department of Homeland Security, *Overview of Risks Introduced by 5G Adoption in the United States*. Cybersecurity and Infrastructure Security Agency, 2019.

Uren, T., "The technical reasons why Huawei is too great a 5G risk", Huawei and Australia 5G Network, report 8/2018, 2018.

United Kingdom Foreign Secretary, "Foreign Secretary's statement on Huawei", last accessed 25 April 2020, https://www.gov.uk/government/speeches/foreign-secretary-statement-on-huawei

United Nations, *Vienna Convention on the Law of Treated 1969*, Vienna: 2005.

United States, Congress House Select Committee on Intelligence. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. Congressional Publications, 2012.

United States, Department of Commerce, *Addition of Certain Entities to the Entity List and Revision of Entries on the Entity List* – Docket No, 190814-0013 Federal Register Vol 84, No 162. Bureau of Industry and Security, Commerce: 2019.

Wendy Dobson. *Living with China : A Middle Power Finds Its Way*, (Toronto: University of Toronto Press, 2019), 120.

World Trade Organization, "The General Agreement on Tariffs and Trade", Geneva: 1986.

World Trade Organization, "Members and Observers", last accessed 1 May 2020, https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm