David Sparling

das816@mail.usask.ca

University of Saskatchewan

Johnson-Shoyama Graduate School of Public Policy

Master of Public Policy Program

Five Eyes, 5G: Huawei and Telecoms Cybersecurity Procedures in Canada

1,498 words

Within the next two years, the Government of Canada will regulate the construction of infrastructure to facilitate the transition to fifth-generation (5G) telecommunications networks. The evolution of Canada's telecommunications networks will require a substantial increase in the number of cellular sites to realize the promise of faster downloads and an enhanced web of telecoms coverage.[1] This digital infrastructure project would be accelerated through the participation of Chinese megacorporation Huawei, an international telecoms leader that provides equipment at cheaper rates than competitors.[2] However, including Huawei in the construction of 5G infrastructure could isolate Canada from allies in the influential Five Eyes intelligence-sharing network and expose Canada to potential cyber threats enabled by Huawei technology.[3] Considering the policy importance of 5G infrastructure integrity, the digital challenges posed by Chinese corporations like Huawei, and the importance of the Five Eyes network to Canadian security interests, the federal government should bar Huawei from Canada's 5G networks until a revised screening procedure incorporating Five Eyes allies is established.

The transition to fifth-generation networks has the potential to be a major boon to Canada's digital economy. Minister of Innovation, Science and Economic Development Navdeep Bains has stated that the transition will create tens of thousands of new jobs and propel Canada to global leadership in communications technologies.[4] As outlined by Communications Research Centre Canada, 5G technology offers advancements for the connectivity, latency, and bandwidth of

---

[1] Robert Fife and Steven Chase, "U.S. Senators Urge Trudeau to Block Huawei from 5G," *The Globe and Mail,* October 12, 2018, https://www.theglobeandmail.com/politics/article-us-senators-urge-trudeau-to-block-huawei-from-5g/.

[2] Melanie Green, "Canada Should Oust Chinese Telecom Huawei, Say Security Experts," *StarMetro Vancouver,* November 8, 2018, https://www.thestar.com/vancouver/2018/11/05/canada-should-oust-chinese-telecom-huawei-say-securityexperts.html.

[3] Fife and Chase, "U.S. Senators Urge Trudeau to Block Huawei from 5G".

[4] M2 Presswire, "Canada's 5G Technology Corridor a Pioneer for Digital Highways," *M2 Presswire,* accessed October 25, 2018, http://go.galegroup.com.cyber.usask.ca/ps/i.do?id=GALE%7CA531565453&v=2.1&u=usaskmain&it=r&p=ITOF&sw=w.

telecommunication devices, revolutionizing the way digital networks interact with one another.[5] Industry leaders portray the evolution to 5G and beyond as a central plank of contemporary national development. Ericsson CEO Borje Ekholm proclaimed: "When we talk about critical national infrastructure, we often talk about roads, bridges and railroads. But future highways will be digital".[6] Given the policy importance ascribed to 5G by both private actors and government officials, the federal government ought to consider risks associated with this transition as an important component of Canadian infrastructure integrity.

Huawei's inclusion in Canada's 5G networks would also complicate Canada's relationship with intelligence allies in the Five Eyes network, the closely-integrated intelligence alliance that allows for unparalleled cooperation on global security between its liberal democratic member states. Most Five Eyes states, including the U.S., Australia and New Zealand, have already banned Huawei from their 5G networks and briefed Ottawa on the security risks associated with Huawei.[7] British telecom BT Group has also moved to remove Huawei equipment from its network, leaving Canada as the only Five Eyes member that has not restricted the Chinese corporation.[8]

In early 2018, the heads of six American spy agencies and three former Canadian intelligence chiefs publicly classified Huawei as a cyber-intelligence threat.[9] In addition, a 2018 study published in *Military Cyber Affairs*[10] alleged that the state-owned Chinese Telecoms corporation

[5] Communications Research Centre Canada, "What is 5G?" *Government of Canada*, accessed October 30, 2018, http://www.crc.gc.ca/eic/site/069.nsf/eng/00077.html/.

[6] M2 Presswire, "Digital Highways".

[7] Robert Fife and Steven Chase, "Five Eyes Spy Chiefs Warned Trudeau Twice about Huawei National-Security Risk," *The Globe and Mail,* December 17, 2018, https://www.theglobeandmail.com/politics/article-five-eyes-spy-chiefs-warn-trudeau-aboutchinas-huawei/.

[8] Fife and Chase, "Huawei National Security Risk."

[9] Fife and Chase, "U.S. Senators Urge Trudeau to Block Huawei from 5G".

[10] The U.S-based journal of the Military Cyber Professionals Organization (double-blind peer reviewed).

had diverted North American internet traffic through strategically-placed 'points of presence' (PoPs).[11] Authors Demchak and Shavitt concluded that these legally-constructed internet access points allowed foreign actors to redirect information-laden internet traffic for the purposes of espionage and intellectual property theft,[12] illustrating a sophisticated effort to use Chinese-built internet infrastructure to subvert North American intelligence safeguards. This conclusion is especially concerning given China's heavily interconnected state and private spheres, and Chinese President Xi Jinping's stated goals to reshape the architecture and norms of the global internet.[13] Furthermore, the summer 2018 revelation that Huawei had established a data-sharing agreement with Facebook demonstrates the company's interest in the personal data of internet users.[14] These insights provide cause for the Government of Canada to re-assess current policies for safeguarding Canadian internet infrastructure.

Although cybersecurity concerns remain high on the agenda in the Sino-Canadian relationship,[15] the Canadian government has not barred Huawei from playing a role in Canada's next-generation telecoms infrastructure. In September 2018, Scott Jones, head of the Centre for Canadian Cyber Security, told a House of Commons committee that Canada's current safeguards were more than adequate for ensuring that Huawei's inclusion would not threaten Canadian

[11] Chris C. Demchak and Yuvall Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking,", *Military Cyber Affairs* 3, no. 1 (2018): 1, http://scholarcommons.usf.edu/mca/vol3/iss1/7.
[12] Demchak and Shavitt, "Leave No Access Point Unexploited".
[13] Adam Segal, "When China Rules the Web," *Foreign Affairs,* September/October 2018, https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.
[14] Sam Sacks, "Beijing Wants to Rewrite the Rules of the Internet," *The Atlantic*, July 18, 2018, https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.
[15] Canadian Security Intelligence Service, *China in the Age of Strategic Rivalry* (Ottawa), 2018, https://www.canada.ca/content/dam/csis-scrs/documents/publications/CSIS-Academic-Outreach-China-report-May-2018en.pdf.

security.[1617] As Canada's top cybersecurity official, Jones' statement can be taken as indicative of the federal government's confidence in Canadian countermeasures against Chinese cyber threats. The Centre's statements referred to the practice of screening telecoms equipment at Huaweifunded "White Lab" facilities to test the company's technology for espionage vulnerabilities.[18] Huawei Canada has maintained that the firm has worked under conditions of full transparency to satisfy cybersecurity concerns.[19] Despite Jones' assurance that Canada has communicated this procedure to the U.S. and Australia,[19] the government's stance on Huawei has already strained Canada's relationship with the Five Eyes network.

The federal government's current approach for reassuring network allies of its commitment to digital security has met with limited success and deserves reconsideration. In September 2018, Senators Marco Rubio and Mark Warner of the American Senate Select Intelligence Committee wrote to Prime Minister Justin Trudeau to urge a ban on Huawei from Canada's 5G networks on national security grounds. Rubio and Warner cited the deep integration of major Chinese companies with the ruling Communist Party, referencing the Chinese government's promotion of Huawei as a 'national champion'.[20] American objections to Huawei's participation in the construction of Canada's 5G networks reflect two broad concerns. First, the senators expressed concerns that Canadian security and data could be compromised by the inclusion of Huawei technology either in the form of deliberate 'back door' systems installed for intelligence-gathering,

---

[16] Government of Canada, "SECU Meeting No. 125," *ParlVU*, accessed November 8, 2018, http://parlvu.parl.gc.ca/XRender/en/PowerBrowser/PowerBrowserV2/20180920/-

[17] /29957?Language=English&Stream=Video&useragent=Mozilla/5.0%20(Macintosh;%20Intel%20Mac%20OS%20X%2010_11_6)%20AppleWebKit/537.36%20(KHTML,%20like%20Gecko)%20Chrome/69.0.3497.100%20Safari/537.36.

[18] ParlVU, "SECU Meeting No. 125".

[19] Fife and Chase. "U.S. Senators Urge Trudeau to Block Huawei from 5G." [19] ParlVU, "SECU Meeting No. 125".

[20] Fife and Chase. "U.S. Senators Urge Trudeau to Block Huawei from 5G."

or through the mandatory compliance with Chinese national intelligences services enforced for Chinese corporations under domestic law.[21] Second, the letter speculated that any inclusion of Huawei technology in Canadian 5G technology could imperil the multinational intelligence sharing enabled by the Five Eyes network.[22]

Canadian officials have committed to avoiding the appearance of bias against China,[23] an increasingly powerful geopolitical player, in decisions related to telecommunications security.[24] Banning Huawei would also escalate the ongoing diplomatic crisis between Canada and China resulting from the late 2018 arrest of Huawei executive Meng Wanzhou and Beijing's subsequent detention of two Canadians.[25] Given this sensitive international situation, the federal government should reconsider its approach to cybersecurity safeguards in relation to the Five Eyes alliance.

The Government of Canada should pursue increased collaboration on digital infrastructure security between the Canadian cybersecurity establishment and partner nations in the Five Eyes network. In order to strengthen Canada's cyber-screening process, the federal government should invite cybersecurity officials from Five Eyes countries to participate in testing Huawei technology at existing White Lab facilities. In addition to involving Canada's intelligence allies more strategically, this policy would operate through established channels that are less likely to provoke a heightened Chinese backlash than an outright ban on Huawei. Until a more collaborative review process is established, the federal government should institute a freeze on Huawei's participation

[21] Fife and Chase. "U.S. Senators Urge Trudeau to Block Huawei from 5G."
[22] Fife and Chase. "U.S. Senators Urge Trudeau to Block Huawei from 5G."
[23] Robert Fife and Steven Chase, "No Need to Ban Huawei in Light of Canada's Robust Cybersecurity Safeguards, Top Official Says," *The Globe and Mail,* September 23, 2018, https://www.theglobeandmail.com/politics/article-no-need-to-ban-huawei-inlight-of-canadas-robust-cybersecurity/?cmpid=rss.
[24] Paul M. Evans, *Engaging China: Myth, Aspiration, and Strategy in Canadian Policy from Trudeau to Harper* (Toronto: University of Toronto Press, 2014), 103.
[25] Robert Fife and Steven Chase, "Huawei National Security Risk."

in the development of Canada's 5G networks. The transition to 5G is a vital policy concern with implications for critical infrastructure integrity and Canada's multilateral intelligence-sharing capabilities. All decisions related to Canada's 5G development should therefore be considered based on national security imperatives in addition to economic considerations.

References

Canadian Security Intelligence Service. *China in the Age of Strategic Rivalry*. Ottawa, 2018. https://www.canada.ca/content/dam/csis-scrs/documents/publications/CSIS-Academic-OutreachChina-report-May-2018-en.pdf.

Communications Research Centre Canada. "What is 5G?" *Government of Canada*. Accessed October 30, 2018. http://www.crc.gc.ca/eic/site/069.nsf/eng/00077.html.

CTV News. "Former CSIS Director, Defence Minister Urge Feds to Bar Huawei from 5G." *CTV News,* October 20, 2018. https://www.ctvnews.ca/politics/former-csis-director-defence-ministerurge-feds-to-bar-huawei-from-5g-1.4142425.

Demchak, Chris C. and Yuvall Shavitt. "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking." *Military Cyber Affairs* 3, no. 1 (2018): 1-9. http://scholarcommons.usf.edu/mca/vol3/iss1/7.

Evans, Paul. *Engaging China: Myth, Aspiration and Strategy in Canadian Policy from Trudeau to Harper*. Toronto: Toronto of University Press, 2014.

Fife, Robert and Steven Chase. "No Need to Ban Huawei in Light of Canada's Robust Cybersecurity Safeguards, Top Official Says." *The Globe and Mail,* September 23, 2018. https://www.theglobeandmail.com/politics/article-no-need-to-ban-huawei-in-light-of-canadasrobust-cybersecurity/?cmpid=rss.

Fife, Robert and Steven Chase. "U.S. Senators Urge Trudeau to Block Huawei from 5G." *The Globe and Mail,* October 12, 2018. https://www.theglobeandmail.com/politics/article-ussenators-urge-trudeau-to-block-huawei-from-5g/.

Fife, Robert, and Steven Chase. "Five Eyes Spy Chiefs Warned Trudeau Twice about Huawei National-Security Risk." *The Globe and Mail,* December 17th, 2018. https://www.theglobeandmail.com/politics/article-five-eyes-spy-chiefs-warn-trudeau-aboutchinas-huawei/.

Government of Canada. "SECU Meeting No. 125." *ParlVU.* Accessed November 8, 2018. http://parlvu.parl.gc.ca/XRender/en/PowerBrowser/PowerBrowserV2/20180920/-1/29957?Language=English&Stream=Video&useragent=Mozilla/5.0%20(Macintosh;%20Intel%20Mac%20OS%20X%2010_11_6)%20AppleWebKit/537.36%20(KHTML,%20like%20Gecko)%20Chrome/69.0.3497.100%20Safari/537.36.

Green, Melanie. "Canada Should Oust Chinese Telecom Huawei, Say Security Experts." *StarMetro Vancouver,* November 8, 2018. https://www.thestar.com/vancouver/2018/11/05/canada-should-oust-chinese-telecom-huaweisay-security-experts.html.

M2 Presswire. “Canada's 5G Technology Corridor a Pioneer for Digital Highways.” *M2 Presswire*. Accessed October 25, 2018. http://go.galegroup.com.cyber.usask.ca/ps/i.do?id=GALE%7CA531565453&v=2.1&u=usaskmain&it=r&p=ITOF&sw=w.

O’Neill, Andrew. “Australia and the ‘Five Eyes’ Intelligence Network: The Perils of an Asymmetric Alliance.” *Australian Journal of International Affairs* 71, no. 5 (2017): 529-543.

Sacks, Sam. “Beijing Wants to Rewrite the Rules of the Internet.” *The Atlantic*, July 18, 2018. https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-tradecyber/563033/.

Segal, Adam. “When China Rules the Web.” *Foreign Affairs*, September/October 2018. https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web.