Parsons, Christopher

Book

Huawei and 5G: clarifying the Canadian equities and charting a strategic path forward

Reference: Parsons, Christopher (2020). Huawei and 5G: clarifying the Canadian equities and charting a strategic path forward. [Toronto] : Munk School of Global Affairs & Public Policy, University of Toronto. https://citizenlab.ca/wp-content/uploads/2020/12/Report133-huaweiand5g.pdf.

HUAWEI & 5G

Clarifying the Canadian Equities and Charting a Strategic Path Forward

By Christopher Parsons

DECEMBER 8, 2020
RESEARCH REPORT #133

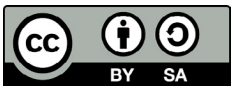
munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

This page is deliberately left blank

Copyright



Electronic version first published by the Citizen Lab in 2020. This work can be accessed through https://citizenlab.ca.

Document Version: 1.0

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a "mixed methods" approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

About the Author

Christopher Parsons is currently a Senior Research Associate at the Citizen Lab, in the Munk School of Global Affairs & Public Policy with the University of Toronto. He received his Bachelor's and Master's degrees from the University of Guelph and his PhD from the University of Victoria.

Acknowledgements

I would like to extend my deepest gratitude and thanks to the people and organizations that have shared their thoughts, expertise, and time with me over the course of this project.

I want to specifically thank Ronald Deibert, Tamir Israel, and Josh Gold for providing support, feedback, and reviews of this report. I would also like to thank the individuals who reviewed drafts of this report but whom cannot be identified for professional reasons. All remaining errors are my own.

Miles Kenyon and Mari Zhou have been instrumental in managing the production of this report, and it was copyedited by Joyce Parsons of Stone Pillars Editing and Consulting. The cover illustration is by Ryookyung Kim and the interior layout is by Mari Zhou.

I had the benefit of participating in a US State Department International Visitor Leadership Program (Cybersecurity) in 2018, which helpfully exposed me to how American civil society, different levels of government, and businesses have reflected on security issues that are linked to infrastructure technologies such as 5G. Those discussions deeply informed some of my early thinking of 5G national security challenges as well as suggested why many popular solutions to such challenges do not adequately take all stakeholders into consideration. In addition to the professionals who graciously donated their time to speak with me during and following that Program, I'm deeply thankful to Claudia L. Valladolid for supporting my nomination to the Program, to my fellow participants Jeremy Depow, Wayne Ewasko, Pierre Paul-Hus, and Karine Pontbriand for the conversations and debates that took place over our travels, and to Virgil Cioflec for gracefully managing the logistics of ensuring we got to our meetings and events on time.

I'm also grateful to the academics, journalists, and organizers of public events who have provided me with spaces to discuss aspects of this report. In particular, I want to thank Michael Geist for hosting me on his *Lawbytes* podcast, which is where I first started to comprehensively articulate the challenges facing Canada as it adopts 5G networking technologies. I also deeply appreciate the opportunity to have spoken about this project at the University of Toronto's Identity, Privacy & Security Institute and at the Canadian Council on International Law, as well as to participants at the Canadian Cyber Dialogue and in other private venues.

Finally, I want to extend my thanks and appreciation to the many individuals in government who have spoken with me about this project but who, for professional reasons,

cannot be identified. This work is stronger for your directness and your patience in explaining different facets of 5G networking technologies as they pertain to security, politics, and power.

This work was supported by the Sigrid Rausing Trust, John D. and Catherine T. MacArthur Foundation, and Open Society Foundations, whose generous funding made this report possible. It was undertaken under the supervision of Prof. Ronald Deibert.

Corrections and Questions

Please send all questions and corrections to the author directly at:

chris@citizenlab.ca

Suggested Citation

Christopher Parsons. “Huawei and 5G: Clarifying the Canadian Equities and Charting a Strategic Path Forward,” Citizen Lab Research Report No. 133, University of Toronto, December 2020.

Contents

Table of Information Boxes

Table of Acroynoms

4G	Fourth Generation
5G	Fifth Generation
6G	Sixth Generation
CCTX	Canadian Cyber Threat Exchange
CFO	Chief Financial Officer
CIA	Confidentiality, Integrity, and Availability
CPC	Communist Party of China
CRTC	Canadian Radio-television and Telecommunications Commission
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CWTA	Canadian Wireless Telecommunications Association
EPO	European Patent Office
EU	European Union
FCC	Federal Communications Commission
GAC	Global Affairs Canada
GCHQ	Government Communications Headquarters
HCSEC	Huawei Cyber Security Evaluation Centre
IA	Information Assurance
IoT	Internet of Things
ITU	International Telecommunication Union
JPO	Japan Patent Office
NCSC	National Cyber Security Centre
NSA	National Security Agency
NSICOP	National Security and Intelligence Committee of Parliamentarians
NSIRA	National Security and Intelligence Review Agency
R&D	Research and Development
SLA	Service Level Agreement
UK	United Kingdom
USPTO	United States Patent and Trademark Office
VI	Virtualized Infrastructure
VNF	Virtualized Network Function
WTO	World Trade Organization

Director's Foreward

Our lives today are completely dependent on a vast technological ecosystem. The devices we carry around with us and which we use to interact with each other through this technological ecosystem send electronic signals through radio waves or cables which are transmitted through a physical infrastructure of routers, servers, cell towers, and data farms, in some cases spread throughout multiple countries. Each step along the way of this complex, distributed ecosystem are numerous businesses upon whose services we depend, including Internet service providers, cable companies, cell service providers, and telecommunications firms as well as the various hardware and software manufacturers supporting them all. How those businesses construct their services and according to whose rules matters enormously for consumers and for national security.

One of the most contentious cases in recent memory around such concerns involves the China-based communications equipment manufacturer, Huawei. Thanks primarily to its affordable pricing, Huawei equipment has proliferated across the globe, and is now deeply embedded in many older generation cell network infrastructures. As more advanced 5G cellular services have gradually been rolled out, Western governments have raised concerns about the possibility that Huawei may have designed secret “back doors” in their technology which would provide China’s security agencies a toe-hold into 5G networks from which to conduct espionage, disrupt communications, or even destroy physical systems.

To be sure, these are appropriate concerns. All companies based in China must comply with China’s broad cyber security laws, which require them (among other things) to share data with China’s security services upon request. Given that 5G networks will be deeply embedded in many critical infrastructures (not to mention the Internet of Things) the vulnerabilities posed by such “back doors” is an ominous threat to society, economics, and politics. Any technology vendor based in China selling services abroad can expect to face such scrutiny for these reasons.

Although valid, these concerns are not unique to China or China-based companies. The history of communications technologies is full of episodes of governments of all sorts cajoling or compelling companies that build or operate infrastructure to insert vulnerabilities to advance intelligence operations. Indeed, as the Snowden disclosures showed, the U.S. National Security Agency and its Five Eyes allies have for years secretly exploited “back doors” of their own design. They also withheld from vendors and the

public information they possessed (and exploited) about flaws in software and hardware that gave them privileged access to company data (including, ironically, around Huawei's equipment).

Christopher Parsons' report helps us understand and navigate these issues with necessary nuance and appropriate attention to details. His report provides a comprehensive tour d'horizon of all of the relevant issues involved in the "Huawei" debate, including legitimate concerns about the safety and security of its equipment and services across a wide range of political, economic, and security perspectives. But in doing so he goes much further than the debates' current myopic focus on China. He reminds us that the appropriate way to address the issues raised by Huawei and 5G equipment as a whole is to start from the ground up and develop a comprehensive public policy for telecommunications infrastructure as a whole. This report is a timely and much welcome mature intervention in a debate that is often fraught with nationalist hysteria and misinformation.

– **Ron Deibert**, Director of the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto.

Executive Summary

Communications technologies are always bound by politics. The ability to communicate more quickly, decode other parties' secret communications, interfere with the integrity of communications, or control what communications infrastructures are available can empower governments and corporations alike. The rise of the fifth generation (5G) mobile broadband cellular technology has brought all of these issues into stark relief as governments, telecommunications providers and vendors, security experts, academics, and citizens have increasingly questioned whether next-generation networks can be trusted to provide reliable, secure, and robust service.

Bringing many of these questions into focus has been the gradual loss of North American capabilities to independently conduct domestic research and development, and to produce, full-scale 5G communications systems and infrastructures that are promised to power the next generation of economic growth. In tandem with the rise of the Chinese company Huawei as a leading telecommunications vendor for 5G systems and China's increasing willingness to forcibly assert its interests internationally, governments in Australia, Canada, New Zealand, the United Kingdom, the United States (the 'Five Eyes' security and intelligence alliance), as well their European allies, have publicly worried and debated about the implications of their nations' telecommunications networks being substantively composed of products manufactured, sold, and maintained by Huawei. Publicly, those concerns have tended to be similar. Some quieter concerns have surrounded whether Huawei has fairly acquired all of the intellectual property it has used to develop its technologies and, more broadly, the business and political influence risks associated with Huawei becoming the world's predominant telecommunications vendor. Some concerns have been raised more loudly about whether the Chinese government could compel Huawei to modify its technologies to facilitate cyber-espionage or disruption operations that could potentially threaten national economies, undermine military capabilities, or otherwise weaponize Western and Western-allied countries' communications networks.

The actual evidence that supports many of these concerns tends to be somewhat murky. This is especially the case when it comes to the Canadian debates concerning Huawei and 5G technologies. This report, "Huawei and 5G: Clarifying the Canadian Equities and Charting a Strategic Path Forward," draws exclusively on open-source reporting to clarify the concerns, assess their seriousness, and outline possible mitigations. But, perhaps most substantially, the report asserts that Canada does not have a 'Huawei problem' per se. Instead, Canada has a 5G strategy problem that is linked to the Government of Canada lacking a principle-driven set of integrated industrial, cyber security, and foreign policy

strategies that directly and meaningfully address the challenges raised by the current and expected 5G landscape. In essence, the Huawei problem should really be reframed as a problem about the Government of Canada's ongoing failure to coordinate across and outside of government to develop a cohesive approach to secure communications infrastructures regardless of whether the vendors powering those infrastructures are based in China, Korea, Norway, or Sweden.

The first three parts of this report provide a background on 5G technologies and its prospective deployments in Canada, on the Chinese telecommunications vendor Huawei, and on the stances that Five Eyes countries have taken toward Huawei and other Chinese telecommunications vendors. More specifically, **Part 1** of this report provides a brief background to 5G technologies in Canada and emphasizes how early decisions concerning the choice of 5G vendors can make it challenging and expensive for telecommunications providers to switch equipment vendors during mid- and late-stages of 5G deployments. **Part 2** outlines key features of Huawei. It recognizes that Huawei has massively invested in research and development, to the effect that the company has accumulated a large volume of key patents that underlie 5G technologies, and it briefly recounts many of the concerns that Western governments have raised concerning the prospect that the Chinese government could influence the company. This part of the report also acknowledges the difficulties in assessing the accuracy of Western governments' concerns based on their common failure to publicly present reliable evidence that would support their security- and influence-based worries. **Part 3** discusses the varied and changing stances that Australia, Canada, New Zealand, the United Kingdom, and the United States have taken toward Huawei. Whereas some of these countries have, as at the time of writing, formally banned Huawei or are in the process of requiring at least some of the company's networking equipment be removed from national networks (Australia, United Kingdom, United States), New Zealand has adopted an ostensibly vendor-neutral security assessment process, while Canada has delayed making a decision as to whether to permit, ban, or partially ban Huawei from selling 5G technologies to Canadian telecommunications companies.

Parts four through seven tease out a range of concerns that Canadian agencies have raised about Huawei and its products in Canada and by our closest diplomatic and military allies. **Part 4** takes up questions about the propriety of Huawei's intellectual property portfolio, the company's dominance in the 5G space, and allegations that the company has benefited from state- or corporate-driven corporate espionage. After recognizing that at least some of the allegations appear to be grounded in verifiable fact, a set of mitigation actions are proposed. First, Canada should adopt a comprehensive national approach to address all cases of foreign corporate espionage to guarantee that

such illicit activity can be prevented or sanctioned, regardless of the company alleged to have carried it out or to have benefited from such activities. Second, Canada could deliberately increase research and development funding for Huawei's competitors—such as Ericsson and Nokia—as well as to Canadian universities to conduct basic research related to next-generation telecommunications. Third, defensive security briefings could be provided to Canadian universities, which generate intellectual property pertaining to next-generation technologies. These briefings could help universities develop and implement public policies intended to mitigate any risks that their research partnerships might jeopardize Canadian economic or national security. Finally, the Government of Canada could more prominently engage with standards bodies to, at least in part, guarantee that such standards have security principles baked in and enabled by default; such efforts could include allocating tax relief to corporations, as well as funding to non-governmental organizations or charities, so that Canadians and Canadian interests are more deeply embedded in standards development processes.

Part 5 accounts for some of the monopoly and trade-related concerns linked with Huawei and with the company being domiciled within China. Specifically, Huawei benefits from trade policies fostered by the Chinese government with the effect that the company is able to compete globally in ways that are difficult for their competitors to match. This uneven competitive playing field includes the presence of Chinese trade barriers that inhibit non-Chinese telecommunications vendors from widely selling products into China and the availability of state-backed, low-interest loans for Huawei's customers. Broadly, these benefits may increase the likelihood that Huawei could become the dominant global telecommunications vendor and, by extension, leave countries such as Canada more likely to be dependent on Huawei in the next stages of 5G development and future 6G deployments. Such dependence would also heighten the security risks posed to Canadian telecommunications companies if these companies predominantly purchase Huawei equipment that possesses either unintentionally or deliberately inserted vulnerabilities. Finally, as China becomes increasingly assertive internationally, it might use any country's dependence on Chinese telecommunications vendors' products as a bargaining chip in diplomatic or trade negotiations. At least some of these challenges might be mitigated by the Canadian government working with allies to appeal to the World Trade Organizations about financial benefits Huawei enjoys from the Chinese government's policies, and to reduce potential risks linked with vendor lock-in by promoting a more vibrant telecommunications vendor community, and thus ensuring that national telecommunications networks can be serviced by a range of companies; these measures could reduce the ability of any country to use their vendors' products as leverage in either bilateral or multilateral negotiations or disputes.

Part 6 attends to what have been the core set of concerns raised about Huawei's products: that its technologies might possess incidentally or deliberately inserted vulnerabilities that the Chinese government or parties operating on its behalf could exploit to the detriment of Canadian interests. This part is, almost by necessity, somewhat speculative as relatively little public evidence has been provided by any government to confirm the assertions that the Chinese government has forced vulnerabilities into Huawei products; most of the open-source evidence of security deficiencies in the company's products, to date, has emerged from the United Kingdom's Huawei Cyber Security Evaluation Centre. After outlining how such vulnerabilities could prospectively be used to enable either espionage or disruption activities, a set of made-for-Canada mitigations are outlined. These focus on three sets of proposals. First, Canadian information assurance operations could be expanded. Such operations would be used to intensively assess products sold by Huawei—as well as other telecommunications vendors—as a way to reduce the likelihood that they contain accidentally or deliberately injected vulnerabilities that could be used to negatively affect Canadians or their governments. Such information assurance operations might be coordinated with close allies to comprehensively assess the security properties of many vendors' networking appliances and other critical infrastructures. Second, security and foreign intelligence operations might be conducted by the Canadian Security and Intelligence Service and Communications Security Establishment, perhaps sometimes with the involvement of the Royal Canadian Mounted Police as appropriate, to increase the costs of secretly inserting vulnerabilities into networking appliances as a way of dissuading any government from tampering with Canadian critical infrastructure. Third, the Canadian government could adopt policies that are designed to make it more difficult to leverage vulnerabilities in 5G appliances to the detriment of Canadians. Such policies might include, as an example, forcefully advocating for the development and integration of strong end-to-end encryption into the Internet of Things and end-point software systems so that compromising 5G networking appliances will not necessarily lead to the revelation of the contents of communications or automatically confer the ability to tamper with the content of those communications.

Part 7 takes up the broader issue of the state of China's rule of law. The Chinese government has sought to improve on its citizens' legal literacy to legitimize the government's activities. At the same time, the Chinese Communist Party and key national security organs of the Chinese state remain elevated above the reach of the courts. The effect of this, in tandem with national security legislation that was passed in 2017, is that should Huawei be compelled to modify its products, the company's ability to resist such pressures in Chinese courts are unlikely to succeed. Consequently, any effort by Canada or its allies to mitigate the risks associated with the Chinese government exercising its domestic powers on Huawei are most likely to take place in international fora where

the Chinese government can be pressured into demonstrating robust domestic rule of law, if only so international companies can be assured of the trustworthiness of Chinese products as China seeks to grow its export markets. In a worst case, Canada and its allies may simply need to develop strategies that anticipate Huawei being forced to modify its products and develop robust information assurance programs to shame the company, and Chinese government, while also serving as a way of issuing warnings to any company that has purchased similarly deficient products.

Finally, **Part 8** outlines some key elements of a 5G strategy for Canada. It focuses on why such a strategy should not be designed to solve a Huawei problem, but to ensure the resiliency, security, and availability of all 5G technologies regardless of the vendor that produces them. These elements draw from earlier sections of the report and specifically suggest ways of protecting and developing intellectual property expertise in Canada, ways of building processes to foster a more diverse market of 5G vendors to mitigate many of the risks linked with vendor monocultures, and ways of ensuring that Canada develops a diversified security posture. In this last category, the Canadian government should work with its allies to engage in coordinated assessment of vendors' networking products, similar to the way the United Kingdom's Huawei Cyber Security Evaluation Centre currently operates. Simultaneously, Canada's security intelligence and foreign signals intelligence agencies should focus their efforts on protecting next-generation infrastructures while remaining subject to strict review to ensure that Canadians can trust that these agencies' activities are lawful, proportionate, and necessary; such trust is essential if Canadians are to trust any reviews or public assertions made by Canada's intelligence and security community. And Canadian companies and other external-to-government stakeholders must be involved in any cybersecurity strategy pertaining to 5G, both so that the government can tap into expertise and knowledge outside of government agencies and because the actual next-generation infrastructures will predominantly be privately run and managed: Canada's 5G challenges can only be overcome in partnership with parties outside of government itself.

A Canadian 5G strategy will need to be coordinated across government in partnership with non-government stakeholders, and it should be designed to mitigate the risks associated with how foreign governments could try to exploit the technology to the detriment of Canadians. Adversaries already probe and exploit Canada's existing networking infrastructures on a daily basis, and they will continue to do so into the future regardless of which vendor's products underpin our telecommunications networks. The solution to Canada's 5G problems will not be found in policies that principally address one company. Instead, a robust and vendor-neutral approach is required. It is my hope that this report, in its entirety, sufficiently lays bare why an interwoven set of Canadian experts and organizations is necessary to create and execute Canada's 5G strategy, and why any

effort to address issues linked with Huawei products in isolation will almost certainly fail to functionally address the broad collection of political, technological, and security issues linked to 5G technologies.

Introduction

Communications systems are inherently political. They connect some groups but not others, are deployed unevenly, and have historically been used to tilt the balance of geopolitical conflicts and power. The fifth generation (5G) technology standard for broadband cellular networks is no exception: it promises to bring the Internet of Things (IoT) into reality with the effect of distributing sensors and actuators around the world to benefit consumers, businesses, and governments alike. These sensors will be able to collect data and, in tandem with actuator equipment, enable heightened remote computing and automation: homes might become better attuned to consumer preferences with the effect of reducing energy consumption; factories might be easier to reconfigure with the effect of enhancing productivity; and health care might be better offered across long distances with the effect of reducing government health budgets. If realized, 5G communications technologies could usher in significant social and industrial changes in the coming decades. But for any of these long-term potentials to be realized, 5G technologies must be available, installed, and trusted.

Over the past 18-24 months, hundreds of articles have been written in the press about opportunities and risks associated with 5G technologies. In Canada, many of those risks have focused on the prospect that Huawei—a Chinese telecommunications vendor—might provide equipment for Canadian telecommunications providers. While general worries have circulated for over a decade about the security of Huawei equipment and the potential that it might be used to enable Chinese government surveillance, these worries have become amplified as 5G technologies have come closer to being widely deployed across Canada. Moreover, the deteriorating Canada-China relationship has led many Canadians, as well as some of their elected representatives and members of the media, to further doubt the appropriateness of Huawei equipment powering Canadian 5G networks.

The actual concerns that have been raised about Huawei technologies, however, are routinely murky and multivariate. Some concerns focus on allegations that Huawei has illicitly obtained technical insights from its competitors or could benefit from state-driven espionage. Other allegations raise the prospect that the prevalence of Huawei technologies in Canadian telecommunications networks might grant the Chinese government leverage in future security, economic, or political disputes. But the majority of the allegations tend to revolve around the national security risks associated with Huawei's products and, specifically, whether the products might be sold with deliberately designed backdoors or possess accidental technical vulnerabilities that functionally constitute backdoors. All of these worries are often stated as factual and pressing, but they are

often supported by unclear or vague evidence. This report unpacks all of these issues, presents the available evidence, and proposes mitigations to specific issues as appropriate. Ultimately, however, this report argues that Canada does not need a Huawei policy but, instead, a deliberate and detailed set of federal strategies that account for industrial development, cybersecurity, and foreign policies pertaining to China in particular.

This report begins by providing a high-level overview of 5G deployment in Canada and a brief corporate profile of Huawei, as well as the policies that have been adopted by Canada and its closest military and security allies. Next, it outlines concerns that are linked with Huawei's 5G networking products. Specifically, the report clarifies some of the asserted issues that pertain to intellectual property, monopoly and trading, national security, and broader rule of law issues associated with the Chinese company. Many of the issues raised in this report are prospective, as opposed to existent, problems. Their prospective nature should not cause a reader to discount them: 5G networking equipment will cost billions to deploy and remain in use for a very long time unless huge expenses are incurred to modify which vendors' products are used in national telecommunications networks. When appropriate, possible mitigations to the issues linked with Huawei products—and 5G technologies more broadly—are raised.

The report concludes by arguing that Canada does not have a Huawei problem, per se, but is suffering from the absence of a clear, actionable, and integrated set of strategies that would guide industrial development, cybersecurity, and foreign policy that is linked with 5G technologies and an increasingly assertive Chinese government. The equities at play in the Huawei debate, at their core, are really questions about how the Canadian government can engage with China and vendors from China in light of China's increasingly expansive and belligerent foreign policy during a time when Canada's historical alliances have been under tension. A 'ban Huawei' policy will not remedy Canada's broader need to strategically chart its course domestically and abroad in a rapidly evolving international and technological order. Attention to Huawei, in particular, should not distract the Canadian government from its need to create robust industrial, cybersecurity, and foreign policy strategies that are designed to ensure that Canada can navigate the increasingly polarized world that it finds itself in.

1. Fifth Generation Deployment in Canada

Fifth Generation (5G) wireless communications can entail either building and extending existing Fourth Generation (4G) communications infrastructures (i.e., enhanced mobile broadband) or building new 5G networks that use core networking equipment to specifically enable advanced Internet of Things (IoT) capabilities (i.e., Stand-Alone 5G).[1, 2] Canadian carriers and the Canadian Wireless Telecommunications Association (CWTA) have indicated that Canadian companies will initially deploy infrastructure that employs the enhanced mobile broadband standard. This standard principally requires modifying the edges of networks. Adopting stand-alone 5G, in contrast, requires more substantial changes to the function and structure of telecom companies' networks, including migrating "from their legacy 4G network consisting of proprietary equipment to a virtualized network."[3] The GSM Association notes that of the global telecommunications companies that it surveyed:

> … there are many challenges and risks in migrating a legacy network to a fully virtualized network. First, ensuring carrier grade SLA (Service Level Agreement) on IT platform is a great challenge, for example five 9s availability. *This also leads to potential lock-in to specific IT vendors as only few vendors would be able to provide telco-grade solutions.* There is also challenge in enlarged base of stakeholders and resulting integration of products. Finally, the cost can increase if VNF (Virtual Network Function) and VI (Virtualized Infrastructure) managers are proprietary.[4]

In part, the risks and costs of migration will cause most carriers to first adopt enhanced mobile broadband and will only integrate stand-alone 5G as virtualization and pushing computing into the cloud becomes more feasible. To date, the Canadian government held one spectrum auction, in 2019, for low-band spectrum allocated to 5G,[5] and a

---

1 Jill C. Gallagher and Michael E. DeVine. (2019). "Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress," *Congressional Research Service*. Available at: https://fas.org/sgp/crs/misc/R45485.pdf.

2 5G networks will rely on up to three swathes of the mobile spectrum to provide reduced latencies and faster data throughput. Low band spectrum (sub-1GHz) is best for supporting widespread coverage of 5G; mid-band spectrum (1GHz-6GHz) will provide additional capacity and coverage; and high-band Millimetre Wave (MMW) can provide ultra-high bandwidth speeds. Each spectrum band has different characteristics. Low-band spectrum can penetrate walls, glass, and other surfaces, whereas mid-band spectrum is less able to penetrate through surfaces. MMW is significantly unable to penetrate through surfaces. For more, see: Jill C. Gallagher and Michael E. DeVine. (2019). "Fifth-Generation (5G) Tele-communications Technologies: Issues for Congress," Congressional Research Service. Available at: https://fas.org/sgp/crs/misc/R45485.pdf.

3 GSMA. (2018). "5G Implementation Guidelines," *GSMA*. Available at: https://www.gsma.com/futurenetworks/wiki/5g-implementation-guidelines/.

4 GSMA. (2018). "5G Implementation Guidelines," *GSMA*. Available at: https://www.gsma.com/futurenetworks/wiki/5g-implementation-guidelines/. Emphasis not in original.

5 Emily Jackson. (2019). "Canadian wireless operators spend $3.5B in 5G spectrum auction; Rogers

mid-band spectrum auction (i.e., 3500MHz) is planned for mid-2021.[6] A high-spectrum auction will take place following the mid-band auction.

Information Box 1: Vendor Lock-In

There is a risk that the vendors that the Canadian carriers use in the first stage of 5G deployment—enhanced mobile broadband—may increase the likelihood of vendor lock-in or subsequent expenses, depending on government policies. Such lock-in is likely given that vendors' own products tend to be deliberately designed to interoperate, but they simultaneously tend to interope rate poorly (if at all) with other vendors' 5G networking products. Specifically, lock-in combined with any policies that forbid an equipment manufacturer from selling core networking equipment could force Canadian companies to either retrofit their equipment or work with vendors to ensure that core 5G virtualized systems are entirely compatible with vendors' products that are used along the edges of the network. This situation means that any policies that approve Huawei equipment for enhanced mobile broadband, when supplemented with potential future policies that could prevent companies from using Huawei for stand-alone 5G, could impose costs on companies that had previously integrated Huawei equipment in enhanced, mobile, broadband networks.

In Canada, Telus' existing non-5G networks are dominated by Huawei equipment and Bell Canada's existing non-5G networks have significant amounts of Huawei equipment. Removing the Chinese company's equipment would allegedly cost Telus between $500 million and $1 billion dollars, and hundreds of millions for Bell.[7] Rogers Communications uses less Huawei equipment in their existing networks. As of writing, Telus has opted to use Ericsson and Nokia equipment, and Rogers and Bell have opted for Ericsson equipment for their respective 5G networks. Both Telus and Bell have, however, left open the option to use Huawei equipment if the Canadian government permits.

buys most as Bell sits out," *Financial Post*. Available at: https://business.financialpost.com/telecom/canadian-wireless-operators-spend-3-5b-in-5g-spectrum-auction-rogers-buys-most-as-bell-sits-out.

6 Tom Li. (2020). "Canada delays key 3500MHz 5G spectrum auction to mid-2021," *IT World Canada*. Available at: https://www.itworldcanada.com/article/canada-delays-key-3500mhz-5g-spectrum-auction-to-mid-2021/431801.

7 Deana Kjuka. (2018). "Canadian telecoms face $1 Billion cost to remove Huawei gear, media report says," *The Toronto Star.* Available at: https://www.thestar.com/business/2018/12/08/canadian-telecoms-face-1-billion-cost-to-remove-huawei-gear-media-report-says.html.

2. What Is(n't) Huawei?

Huawei is a private Chinese company and one of the world's largest manufacturers of telecommunications equipment. The company is one of the handful of companies globally that can develop and deploy the 5G equipment that telecommunications providers need to provide 5G networks and services to their customers. Huawei can produce every element of a 5G network, from the radios used in mobile phones, the mobile phones themselves, and all elements on the carrier-side of the networking infrastructures inclusive of virtualization functions.[8] Huawei's industrial capabilities, in tandem with the company's strong service culture and ability to sell products below the cost of their competitors, have enabled the company to sell its networking equipment throughout the world.

Information Box 2: Huawei's Patent Holdings

Part of the reason that Huawei can produce everything that is involved in establishing a 5G network is that the company has been prominently involved in the 5G standards-setting process. As noted by Parv Sharma of Counterpoint Research, Chinese companies—and especially Huawei[9]—have been active in "developing 5G standards and acquiring related IP."[10] These investments in 5G-based research and development have led to Chinese stakeholders owning approximately 10% of "5G-essential" patents.

While Chinese stakeholders have filed a large volume of 5G-related patents, some analysts have questioned the quality of the patents[11] and have raised specific doubts that the patents are as closely linked to innovation as may be imagined at first glance.[12] The gold standard for quality patents are so-called 'triadic patents', which involve successfully registering patents with the Japan Patent Office (JPO), the United States Patent and Trademark Office (USPTO), and the European Patent Office (EPO). Chinese companies

8 The company's ability to provide these products has come under pressure as the United States has expanded its sanctions regime.

9 Other dominant Chinese actors include: China Mobile, ZTE, and China's Academy of Telecommunications Technology (CATT).

10 Parv Sharma. (2018). "5G Ecosystem: Huawei's Growing Role in 5G Technology Standardization," *Counterpoint Research*. Available at: https://www.counterpointresearch.com/huaweis-role-5g-standardization/.

11 Elsa B. Kania. (2019). Transcript for May 27, 2019. *The Current.* Available at: https://www.cbc.ca/radio/thecurrent/the-current-for-may-27-2019-1.5148981/may-27-2019-episode-transcript-1.5151738.

12 Elsa B. Kania. (2019). "Why Huawei Isn't So Scary," *Foreign Policy.* Available at: https://foreignpolicy.com/2019/10/12/huawei-china-5g-race-technology/.

have historically obtained far more domestic Chinese patents than triadic patents. Triadic patents "are considerably more expensive than domestic applications. They are harder to obtain [than Chinese patents], and in some cases, can take up to five or six years to process."[13] However, the time delta between filing for triadic patents and receiving them may conceal the quality of the patents filed by Huawei and other Chinese companies and innovators in international fora; it is possible that Huawei and other Chinese companies do, in fact, hold a vast set of important and high-quality 5G-related international patents in addition to domestically-filed ones.

The American government, amongst others, has raised concerns about the relationship between Huawei and the Chinese government for over a decade. As an example, the US House of Representatives Permanent Select Committee on Intelligence raised the following concerns in 2012:

- a lack of clarity concerning the relationship between Huawei and the Chinese government
- a lack of clarity concerning the role of the Chinese Communist Party Committee(s) within Huawei
- a lack of clarity concerning the extent to which Huawei has dealings with the Chinese military or intelligence services.[14]

Many of these concerns, at their core, arise from a general lack of public understanding about the roles of Party Committees within private companies combined with the ways Chinese state policies are sometimes handed down through combinations of hard and soft law. The result is that some Chinese companies, including Huawei, are regarded as potentially susceptible to direct and indirect state compulsions, which could potentially be to the detriment of the security or privacy interests of international users of such companies' products and services.

While the concerns that the US House Intelligence committee raised hold some merit and have been amplified by reporting about the difficulties of understanding the ownership structure and potential Party influence within Huawei through Party Committees,[15] the

13 China Power Team. (2019). "Are patents indicative of Chinese innovation?" *China Power*. Available at: https://chinapower.csis.org/patents/.

14 Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger. (2012). "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," *United States House of Representatives, 112th Congress—Permanent Select Committee on Intelligence.* Available at: https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96.

15 See: Ashley Feng. (2019). "We Can't Tell if Chinese Firms Work for the Party," *Foreign Policy.* Available at: https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/; Elsa Kania. (2018). "Much ado about Huawei (part 2)," https://www.aspistrategist.org.au/much-ado-huawei-part-2/; Raymond Zhong. (2019). "Who Owns Huawei? The Company Tried to Explain. It Got Complicated," *New York Times*. Available at: https://www.nytimes.com/2019/04/25/technology/

2012 US governmental report lacks a conclusive answer about the substantive impact of such influences. This having been said, the report does indicate that persons operating the China-domiciled elements of Huawei held significant sway over the branch of the company that had been established in the United States. Specifically, the parent company had "set general terms for operations in the United States" and contracts that the United States subsidiary sought to enter into first had to be approved by staff in China. Further, "in one instance, a contract previously signed by a U.S.-based senior official at Huawei was repudiated by the parent company."[16] When directly asked about the relationship between the United States and China-based businesses, "Huawei failed to provide any further information about the level of coordination between Huawei USA and the parent company."[17] None of these findings clearly demonstrate that the Chinese-domiciled branch of Huawei has a controlling interest over the daily activities of its USA-domiciled branch, but simultaneously, they have cast doubt over the actual independence of the company's American operations with regard to both its parent company and, through that company, direct and indirect pressures from the Chinese government.

In Canada, Huawei representatives have confirmed that they follow Canadian laws and, as such, will not engage in "issues like espionage and pilfering data and all that."[18] However, past company representatives have noted that before they could obtain money for even marketing purposes, they required approval from the China-based executive staff.[19] To date, no Canadian legislative committee has conducted an assessment of Huawei that parallels the one undertaken by the US House of Representatives Permanent Select Committee on Intelligence, though such a report might emerge in the future from the House of Commons Special Committee on Canada-China Relations, the House of Commons Standing Committee on Public Safety and National Security, or the Standing

who-owns-huawei.html; Dan Strumpf and Yifan Wang. (2019). "Huawei Says It Is Employee—'Owned'—But Not Really," *Wall Street Journal.* Available at: https://www.wsj.com/articles/huawei-says-it-is-employee-ownedbut-not-really-11556204552; Xiaojun Yan and Jie Huang. (2017). "Navigating Unknown Waters: The Chinese Communist Party's New Presence in the Private Sector," *The China Review* 17(2), pp. 37-63.

16 Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger. (2012). "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," *United States House of Representatives, 112th Congress—Permanent Select Committee on Intelligence.* Available at: https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96; pages 30-31.

17 Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger. (2012). "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," *United States House of Representatives, 112th Congress—Permanent Select Committee on Intelligence.* Available at: https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=96; pages 30-31.

18 Catharine Tunney. (2019). "Huawei hit with security questions as it unveils high-speed rural internet project," *CBC News* (July 23, 2019). Available at: https://www.cbc.ca/news/politics/huawei-north-high-speed-1.5220354.

19 Based on a public presentation by Scott Bradley, formerly an executive at Huawei Canada.

Senate Committee on National Security and Defence.[20] As of writing, there is no equivalent Canadian public report that assesses whether Canadian Huawei employees behave similarly to their American counterparts, or whether Party Committees exert pressure on the Canadian subsidiary. Broadly, despite protestations to the contrary and the murkiness surrounding the issue, the China-based staffs do appear to exert some degree of influence over at least some corporate activities undertaken by Huawei's foreign subsidiaries. Moreover, even should there be significant independence between Huawei's regional subsidiaries and its China-based parent company, any pressures placed on the parent company by the Chinese government could enable the kinds of espionage activities that the American government has warned about.

Ultimately, it is challenging to assess the worries about relationships between individuals working for Huawei and the Chinese security, intelligence, and defence communities, or the relationships between members of the Chinese Communist Party Committees, the government, and corporate executives. While it is normal for individuals who work in intelligence communities to shift to work in the telecommunications industry, Western states have not clearly shown whether such employment shifts are malign when it comes to Huawei. Instead, governments and legislators have asserted that Huawei operates at the behest or direction of the Chinese government without presenting compelling evidence that the company clearly takes any of its directions from the Chinese military or security and intelligence apparatuses.[21] Simultaneously, efforts to understand who exactly is in control of decision-making at Huawei has been fraught with difficulty, and the effort has left external observers without a clear understanding of who controls Huawei or the effects of that control.[22]

---

20 The Hon. Leo Housakos moved that the Standing Senate Committee on National Security and Defence be authorized to examine and report on the prospect of allowing Huawei Technologies Co., Ltd. to be part of Canada's 5G network when and if the committee is formed and that the committee submit its final report no later than April 30, 2020. See: https://sencanada.ca/en/content/sen/chamber/431/debates/008db_2020-02-18-e#78. To date, no such report has been submitted.

21 Marieke Walsh. (2020). "Canada should stand up to China, ex-Australia PM says," *Globe and Mail.* Available at: https://www.theglobeandmail.com/politics/article-canada-should-stand-up-to-china-ex-australia-pm-says/; Marco Rubio. (2020). "Op-ed: America and its allies must reject China's Huawei and lead on 5G development," *CNBC*. Available at: https://www.cnbc.com/2020/09/03/op-ed-america-allies-must-reject-chinas-huawei-lead-on-5g.html; Alexandra Alper and Idrees Ali. (2020). "Exclusive: Trump administration says Huawei, Hikvision backed by Chinese military," *Reuters.* Available at: https://www.reuters.com/article/us-usa-china-military-exclusive-idUSKBN23V309; See also: Department of Defense. (2020). "Qualifying Entities Prepared in Response to Section 1237 of the National Defense Authorization Act for Fiscal Year 1999 (PUBLIC LAW 105–261)," *United States Government.* Available at: https://media.defense.gov/2020/Aug/28/2002486689/-1/-1/1/LINK_1_1237_TRANCHE-23_QUALIFYING_ENTITIES.PDF.

22 Ashley Feng. (2019). "We Can't Tell if Chinese Firms Work for the Party," *Foreign Policy.* Available at: https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/; Elsa Kania. (2018). "Much ado about Huawei (part 2)," https://www.aspistrategist.org.au/much-ado-huawei-part-2/; Raymond Zhong. (2019). "Who Owns Huawei? The Company Tried to Explain. It Got Complicated," *New York Times.* Available at: https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html; Christopher Balding and Donald C. Clarke. (2019). "Who Owns Huawei?" *Social Sciences Research Network.* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669.

3. Current Stances Held by Five Eyes Countries

Huawei has, generally, been viewed with significant suspicion by security and intelligence agencies within the Five Eyes countries, a set of countries composed of Australia, Canada, New Zealand, the United Kingdom, and the United States of America that routinely cooperate on national security and intelligence affairs. In Australia, Huawei has been banned from participating in the country's national broadband networks and 5G networking infrastructures.[23] The government asserted that these bans were based on security concerns and risks, as opposed to privacy-related worries.[24] Australia has worked to encourage its neighbours, such as the Solomon Islands and Papua New Guinea, to not acquire Huawei backed underseas cables.[25] Huawei has previously proposed creating an evaluation centre in Australia where Huawei equipment could be subject to security assessment prior to being deployed in Australian networks.[26] To date, no such evaluation centre has been established.

In New Zealand, the country's security services have blocked Huawei from supplying mobile network equipment for 5G infrastructures on national security grounds.[27] The government has asserted that all evaluations of 5G infrastructure vendors will be evaluated on the basis of national security, as opposed to upon political calculations.[28] While Huawei has floated the idea of opening an evaluation centre to assuage the Government Communications Security Bureau's (GCSB) concerns around the security of Huawei 5G equipment,[29] as of writing, the de facto ban remains, and no evaluation centre has been created.

---

23 Danielle Cave. (2019). "Australia and the great Huawei debate: risks, transparency and trust," *Australian Strategic Policy Institute.* Available at: https://www.aspistrategist.org.au/australia-and-the-great-huawei-debate-risks-transparency-and-trust/.

24 Jamie Smyth. (2019). "Australia banned Huawei over risks to key infrastructure," *Financial Times.* Available at: https://www.ft.com/content/543621ce-504f-11e9-b401-8d9ef1626294.

25 Rosie Perper. (2019). "Australia snubbed Huawei and completed its undersea cable project to bring high-speed internet to Pacific Islands," *Business Insider.* Available at: https://www.businessinsider.com/australia-snubs-huawei-finishes-undersea-cables-for-pacific-islands-2019-8.

26 Sean Gallagher. (2012). "Huawei: worried about cyber-espionage backdoors? You can look at our code," *Ars Technica.* Available at: https://arstechnica.com/tech-policy/2012/10/huawei-worried-about-cyber-espionage-backdoors-you-can-look-at-our-code/.

27 Jasper Jolly. (2018). "New Zealand blocks Huawei imports over 'significant security risk'," *The Guardian.* Available at: https://www.theguardian.com/business/2018/nov/28/new-zealand-blocks-huawei-5g-equipment-on-security-concerns.

28 Fumi Matsumoto. (2019). "New Zealand's 5G plan 'not a political decision'," *NIKKEI Asian Review.* Available at: https://asia.nikkei.com/Editor-s-Picks/Interview/New-Zealand-s-5G-plan-not-a-political-decision.

29 Tom Pullar. (2019). "Let us into 5G and we could pay millions for NZ cyber lab, says Huawei," *Stuff.* Available at: https://www.stuff.co.nz/business/industries/110090703/let-us-into-5g-and-we-could-pay-millions-for-nz-cyber-lab-says-huawei.

The United Kingdom (UK) has shifted its decision concerning whether to permit or block Huawei from participating in 5G networking infrastructures as a result of changing domestic and international pressures. In 2011, the UK government established the Huawei Cyber Security Evaluation Centre (HCSEC). The HCSEC is a partnership between Huawei and the UK government that is intended to provide assurance that private UK telecommunications networks can safely and reliably integrate and use Huawei equipment. The Centre was created following British intelligence agencies' being notified by BT Group plc (formally British Telecom) that, "core switches installed by Huawei as part of that network were doing an unusual amount of "chattering"[.]"[30] Functionally, the HCSEC is staffed with Huawei employees and overseen by the British government's signals intelligence agency, the Government Communications Headquarters (GCHQ).

The HCSEC has evaluated core and non-core enterprise networking equipment. The Centre's 2018[31] and 2019[32] reports found significant security deficits in how Huawei products were engineered. None of these deficits were linked to compulsions by Chinese state actors but, instead, to an immature security culture within the company's engineering staffs. The technical director of the GCHQ's National Cyber Security Centre went so far as to state that Huawei's security was "very, very shoddy" and had "engineering like it's back in the year 2000."[33]

Huawei equipment remained available for sale in the UK following the HCSEC's assessment that the UK, "would be very vulnerable to be exploited" should the UK and its allies rely solely on networking equipment provided by Huawei and ZTE, another Chinese telecommunications vendor.[34] In January 2020, the UK government laid out a series of rules under which Huawei equipment could be used in UK 5G networks: only up to 35% of the networks could include the company's equipment and their equipment was

30 Amit Katwala. (2019). "Here's how GCHQ scours Huawei hardware for malicious code," *Wired.* Available at: https://www.wired.co.uk/article/huawei-gchq-security-evaluation-uk.

31 Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. "Annual Report 2018: A report to the National Security Adviser of the United Kingdom," *HCSEC.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.

32 Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. "Annual Report 2019: A report to the National Security Adviser of the United Kingdom," *HCSEC*. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

33 Leo Kelion. (2019). "Huawei's 'shoddy' work prompts talk of a Westminster ban," *BBC News.* Available at: https://www.bbc.com/news/technology-47830056.

34 Ryan Browne. (2019). "Former UK spymaster plays down national security fears over Huawei," *CNBC.* Available at: https://www.cnbc.com/2019/10/09/former-uk-spymaster-john-sawers-plays-down-huawei-security-fears.html.

barred from certain critical infrastructure.[35] These positions were reversed, however, in July 2020; no new Huawei 5G equipment can be purchased after December 31, 2020. The changed policy position was anticipated to delay the UK's rollout of 5G by two to three years and at a cost of up to £2 billion.[36] The government presented contradictory reasons for the reversal. Officially, the government justified the newest policy position based upon new advice provided by the National Cyber Security Centre (NCSC), a part of the GCHQ. The NCSC wrote that American sanctions, which were established in May 2020, would prevent Huawei from obtaining US technology and software that was used in Huawei's design and manufacturing of its products, which meant that the NCSC, "no longer considers that the UK will be able to manage the security risks of using affected Huawei technology in our future 5G networks."[37] However, journalists have reported that the government's new policy is linked, behind the scenes, to geopolitics and that the ban on Huawei equipment might be reversed should US sanctions be removed.[38] However, this reversal might be complicated by the House of Commons Defence Committee's call for the removal of Huawei equipment from United Kingdom networks on the asserted basis that the company and Chinese government have colluded with one another in the past.[39]

Government officials and politicians who have been briefed by the United States' intelligence committee have long warned of prospective risks linked to Huawei and other Chinese companies' telecommunications equipment. In 2012, the House Intelligence Committee held hearings on Chinese telecommunications vendors and concluded that Huawei and ZTE posed national security threats.[40] As part of the hearings, Huawei suggested opening a cyber evaluation centre as they had in the UK, only to have the proposal rejected on the basis that "the complexity of hardware and software would

35 Ian Levy. (2020). "The future of telecoms in the UK," *UK Nation Cyber Security Centre.* Available at: https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk.

36 Dan Sabbagh and Lily Kuo. (2020). "Huawei to be stripped of role in UK's 5G network by 2027, Dowden confirms," *The Guardian.* Available at: https://www.theguardian.com/technology/2020/jul/14/huawei-to-be-stripped-of-role-in-uk-5g-network-by-2027-dowden-confirms.

37 National Cyber Security Centre. (2020). "Huawei advice: what you need to know," *National Cyber Security Centre.* Available at: https://www.ncsc.gov.uk/information/huawei-advice-what-you-need-to-know.

38 Toby Helm. (2020). "Pressure from Trump led to 5G ban, Britain tells Huawei," *The Guardian.* Available at: https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei.

39 Defence Committee. (2020). "The Security of 5G," *UK House of Commons.* Available at: https://committees.parliament.uk/publications/2877/documents/27899/default/.

40 Michael S. Schmidt, Keith Bradsher, and Christine Hauser. (2012). "U.S. Panel Cites Risks in Chinese Equipment," *New York Times*. Available at: https://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html. See also: House Permanent Select Committee on Intelligence. (2012). "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecom-munications Companies Huawei and ZTE," *United States Congress.* Available at: https://fas.org/irp/congress/2012_rpt/huawei.pdf.

make it impossible to fully assure that products from the company were not vulnerable to manipulation."[41] Later, in February 2020, US officials revealed that they were particularly concerned by Huawei's alleged decade-long capability to secretly enable its products' lawful interception interfaces; such activations allegedly bypass the controls that are supposed to solely vest control of such interfaces with telecommunications operators.[42] To date, no open-source information has substantiated these allegations.

To offset some security-related concerns linked with 5G technologies in the United States, the Federal Communications Commission (FCC) was tasked with ensuring that all new 5G technologies had security standards built into the technologies themselves in 2016;[43] this was rescinded by the Trump FCC under pressure from industry in 2017.[44] In 2018, legislation was passed, as part of the National Defense Authorization Act, that banned Huawei products (and other Chinese vendors' equipment) from being used by the US government and its contractors[45] with the legislation entering into force in the fall of 2019.[46] In 2019, the FCC voted to bar telecommunications carriers from receiving federal money to expand Internet connectivity if that money would be used to acquire Huawei or ZTE equipment,[47] and in June 2020, it voted to designate Huawei and ZTE Corp as national security threats.[48] The result of government and regulatory action has been to prevent the future sale of Huawei and ZTE equipment for use in American telecommunications

41 Sean Gallagher. (2012). "Huawei: worried about cyber-espionage backdoors? You can look at our code," *Ars Technica.* Available at: https://arstechnica.com/tech-policy/2012/10/huawei-worried-about-cyber-espionage-backdoors-you-can-look-at-our-code/.

42 Bojan Pancevski. (2020). "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *Wall Street Journal*. Available at: https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

43 Federal Communications Commission. (2016). "In the Matter of Fifth Generation Wireless Network and Device Security (PS Docket No. 16-353)," *FCC*. Available at: https://apps.fcc.gov/edocs_public/attachmatch/DA-16-1282A1_Rcd.pdf.

44 Federal Communications Commissioner. (2017). "In the Matter of Fifth Generation Wireless Network and Device Security," *FCC*. Available at: https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0203/DA-17-131A1.pdf. See also: Tom Wheeler. (2018). "Building a secure 5G network without nationalization," *Brookings*. Available at: https://www.brookings.edu/blog/techtank/2018/01/29/building-a-secure-5g-network-without-nationalization/.

45 Timothy B. Lee. (2018). "New law bans US gov't from buying tech from Chinese giants ZTE and Huawei," *Ars Technica*. Available at: https://arstechnica.com/tech-policy/2018/08/trump-signs-bill-banning-feds-from-using-huawei-zte-technology/.

46 Roberta Rampton. (2019). "U.S. government contractors get first look at Huawei ban," *Reuters.* Available at: https://www.reuters.com/article/us-usa-trade-huawei/u-s-government-contractors-get-first-look-at-huawei-ban-idUSKCN1UX1TF.

47 Federal Communications Commission. (2019). "In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs (PS Docket No. 19-351 & No. 19-352)," *FCC*. Available at: https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

48 Federal Communications Commission. (2020). "In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs—Huawei Designation (PS Dock-et No. 19-351)," *FCC.* Available at: https://docs.fcc.gov/public/attachments/DA-20-690A1.pdf; Federal Communications Commission. (2020). "FCC Designates Huawei and ZTE As National Security Threats," *FCC.* Available at: https://docs.fcc.gov/public/attachments/DOC-365255A1.pdf.

networks, while simultaneously placing pressure on allies to similarly ban these companies' 5G technologies.

The Canadian government has mounted a range of investigations and ongoing assessments of Huawei's technologies. In 2012, Ottawa used a national security protocol to indicate to Huawei that the government would prevent the firm from bidding on the government's telecommunications and email network.[49] Press reports revealed that an assistant deputy minister of public national security, within the Public Safety Canada portfolio, had previously raised national security concerns associated with integrating Huawei equipment into Canadian networks, and especially those that may interoperate with networks used by the United States government.[50] Access to information requests seeking information about the government assessments of Huawei's technologies and prospective involvement in espionage activities have, to date, not publicly indicated that the company has been involved in espionage, though all response documents have been very heavily redacted. In addition, Canada—through EWA-Canada[51]—engages in assessments of Huawei products, though with potentially less capacity to influence changes in Huawei's development and security culture as compared to assessments undertaken by the UK's HCSEC.[52]

As of writing, the Canadian government has not formally declared whether it will permit private companies to purchase Huawei 5G equipment and, if so, what security conditions might be applied. As of June 2020, Telus has opted to use Ericsson and Nokia equipment, and Rogers and Bell have opted for Ericsson equipment for their respective 5G networks.[53] Both Telus and Bell have, however, left open the option to use Huawei equipment if permitted by the Canadian government. Government of Canada insiders have

---

49 Associate Press. (2012). "Ottawa set to ban Chinese firm from telecommunications bid," *Associated Press.* Available at: https://www.theglobeandmail.com/news/politics/ottawa-set-to-ban-chinese-firm-from-telecommunications-bid/article4600199/.

50 Ben Makuch. (2014). "Huawei Makes Canada Nervous Too," *Motherboard.* Available at: https://www.vice.com/en_us/article/pgazyy/huawei-has-made-canada-nervous-for-years.

51 EWA-Canada has staff in Canada and Sweden and provides both product- and network-focused cybersecurity services pertaining to Common Criteria, cryptographic certification, supply chain assessment, among other services. For more, see: https://www.intertek.com/cybersecurity/ewa-canada/.

52 Intelligence and Security Committee. (2013). "Foreign involvement in the Critical National Infrastructure: The implications for national security," *United Kingdom*. Available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20130606_ISC_CNI_Report.pdf?attachauth=ANoY7cpUmn279sOigdAcYOZ5afZXPPg8Ll8RqZMzUSJSON5APiCq4_uLfsPw8tX7putc3g458h-cNAeuMH9XuueP4SQOEdL6fI_Qg1dlFKY-NZKPSF21IrRJZ66OHJCIrLimEPy2ZND-uYWGNTkefQzgTa0qhMwhffPrp772DQTp-G9c1DsohEBbT8vzh6FUEZjovG-xsSC7B9jpvu55q-dESkv5DBe9xcZ3-OGyr31LBLW3le4S--ow%3D&attredirects=1, p. 15. The UK's "success in driving significant change in the company has been in no small part due to the reach back the Cell has – and uses – on our behalf. Experience of independent third parties (e.g. EWA Canada) [shows] that they do not have sufficient influence on the larger corporate machine."

53 Tyler Orton. (2020). "Updated: Telus dumps Huawei's 5G tech hours after Bell," *BIV.* Available at: https://biv.com/article/2020/06/updated-telus-dumps-huaweis-5g-tech-hours-after-bell.

suggested that if Huawei products are banned, private companies may not receive any funds to remove previously installed 3G, 4G, or other equipment.[54]

The remainder of this report discusses many of the equities that are at play with regard to permitting, denying, or selectively permitting Canadian telecommunications carriers to utilize Huawei's 5G networking products. Each subsection includes ways that some risks that might be associated with Huawei equipment might be managed or mitigated. Such conclusions are meant to help determine how to engage with Huawei or other foreign telecommunications vendors, but these conclusions should not be regarded as exhaustive.

54 David Ljunggren. (2020). "Exclusive: Canada looks set for a fight over C$1 billion compensation for Huawei gear," *Reuters.* Available at: https://www.reuters.com/article/us-canada-huawei-exclusive-idCAKBN2640KR.

4. Intellectual Property and Commercial Espionage Concerns

A range of actors have raised intellectual property concerns associated with Huawei that are linked to, on the one hand, Huawei's advanced research capabilities and the company's alleged appropriation or unauthorized use of intellectual property and, on the other hand, the prospect that Huawei could benefit from the Chinese government's espionage operations. This section briefly outlines such concerns and then discusses some paths that might mitigate these existing or potential policy problems.

4.1 - Overview of Issues

Huawei invests considerable sums of money to develop new technologies. In China, the company invested a total of $75.7 billion (USD) from 2006-2018[55] and, in Canada, Huawei invested at least $500 million (USD) between 2009-2019.[56] Huawei invested more than $56 million (CAD) in Canadian universities over the course of 2014-2019,[57] with that money supporting university research labs, university scholarships, and other academic-focused research. A minor public controversy around Huawei's academic investments has previously arisen on the basis that some recipients of these investments, "assigned all intellectual property rights to the company," and in other cases, the company licensed, "intellectual property from Canadian university researchers, often giving the company exclusive rights to their publicly funded research."[58] There is no indication, however, that such intellectual property licensing agreements violate any laws or federal rules.

The Canadian Security Intelligence Service (CSIS) has provided briefings to some universities about the risks of academic research outputs that constitute 'dual purpose'

---

55 Huawei. (2018). "Huawei's 2017 Annual Report: Solid Performance and Lasting Value for Customers," Huawei. Available at: https://www.huawei.com/us/press-events/news/2018/3/huawei-2017-annual-report; Wang Zekun. (2019). "Huawei's Investment in R&D Ranks a Leading Position," *Equal Ocean*. Available at: https://equalocean.com/news/201904301915. Total investment was calculated by tabulating spending denoted in the 2017 annual report with that in the Equal Ocean article.

56 Lynn Greiner. (2019). "Huawei boosts R&D spend, hires more in Canada as U.S. tensions rise," *IT World Canada.* Available at: https://www.itworldcanada.com/article/huawei-boosts-rd-spend-hires-more-in-canada-as-u-s-tensions-rise/415248.

57 Peter Armstrong. (2019). "Huawei funds $56M in academic research in Canada. That has some experts concerned," *CBC News.* Available at: https://www.cbc.ca/news/business/huawei-academic-funding-in-canada-1.5372310. While the University of Toronto has received money from Huawei, the Citizen Lab has never benefitted from such funds, nor has anyone at the University of Toronto suggested revisions to this report based on the University's receipt of money from Huawei.

58 Steve Chase. (2018). "How Canadian money and research are helping China become a global telecom superpower," *The Globe and Mail.* Available at: https://www.theglobeandmail.com/canada/article-how-canadian-money-and-research-are-helping-china-become-a-global/.

technologies, or those that could have both civilian- and military-related uses.[59] The CSIS has also warned that China represents, "the most significant and clear" challenge when it comes to espionage targeting Canadian universities.[60] Global Affairs Canada (GAC) has also briefed some academics on risks associated with collaboration with Huawei.[61] It remains unclear what exact research is being funded or the comprehensive rights afforded to Huawei as a result of funding academic research. The Canadian government has not, to date, taken sanctions positions toward Huawei that parallel those of the United States and, as such, Canadian universities are under no requirement to abstain from research funding from Huawei.

In addition to investing in research to generate intellectual property it either owns or licenses, there have been allegations that Huawei has illicitly obtained other parties' intellectual property. As reported by the *Wall Street Journal*,[62] Huawei has been accused of:

- copying Cisco software and manuals, and then reselling them as Huawei products
- stealing Motorola technology, which was used to develop products designed to undercut Motorola's own offerings
- misappropriating trade secrets that compose a "building block of technology that forms signals in 5G networks"
- encouraging a Brazilian telecommunications organization to provide Huawei with competitors' products in order to receive free Huawei equipment
- developing a smartphone camera system despite knowing the system was previously patented
- using copyrighted music on millions of devices without first obtaining the rights to the music
- actively reminding employees to "get foreign data, including confidential information" that included pressuring an American Huawei engineer to obtain information about

59 Sean Silcoff. (2018). "Canada's spy agency cautions universities with research ties to Huawei," *The Globe and Mail.* Available at: https://www.theglobeandmail.com/politics/article-csis-cautions-canadian-universities-about-research-ties-with-huawei/.

60 Douglas Quan. (2019). "'Significant and clear' threat: What Canada's spy chief says about China behind closed doors," *National Post.* Available at: https://nationalpost.com/news/canada/significant-and-clear-threat-what-canadas-spy-chief-says-about-china-behind-closed-doors.

61 See comments made by Mr. Garnett Genius and Prof. Yves Tiberghien at: https://www.ourcommons.ca/DocumentViewer/en/43-1/CACN/meeting-7/evidence#Int-10769928.

62 Chuin-Wei Yap, Dan Strumpf, Dustin Volz, Kate O'Keeffe, and Aruna Viswanatha. (2019). "Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics," *Wall Street Journal.* Available at: https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858.

"how to replicate a robot called Tappy developed by T-Mobile to mimic an ultra-fast human finger and test a smartphone's responsiveness"

- instructing a Huawei engineer to pose as a customer to ultimately obtain CNEX's solid-state disk storage technology
- instructing an American software architect to register fake company names in order to attend an industry conference about collaborative network designs, held by Facebook and to which Huawei was deliberately not invited.

Separately, individuals have been charged with stealing trade secrets to advance Huawei's interests[63] and Huawei has been accused of operating a program designed to encourage (and reward) employees to engage in intellectual property theft. This program allegedly included Huawei establishing, "a special Huawei encrypted internal email address" that employees were told to use when they transmitted sensitive information, and employees were allegedly told that, "they had the responsibility to collect competitor information."[64]

In addition to concerns that are linked directly with Huawei, some state-affiliated Chinese operators also engage in industrial espionage activities that could potentially be designed to benefit domestic companies.[65] These operators' espionage activities can involve stealing intellectual property that, when used by indigenous Chinese companies, sometimes reduce research and development costs and latencies in producing commercial products, systems, and components.[66] Chinese operators have also allegedly stolen business information to assist Chinese companies in their business negotiations.[67] There are no open-source records that indicate that Huawei has clearly or directly benefited from Chinese operators' hacking operations.[68] Nonetheless, the potential prospect for

63 Chuin-Wei Yap, Dan Strumpf, Dustin Volz, Kate O'Keeffe, and Aruna Viswanatha. (2019). "Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics," *Wall Street Journal.* Available at: https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858.

64 Dan Strumpf and Patricia Kowsmann. (2019). "U.S. Prosecutors Probe Huawei on New Allegations of Technology Theft," *Wall Street Journal.* Available at: https://www.wsj.com/articles/u-s-prosecutors-probe-huawei-on-new-allegations-of-technology-theft-11567102622.

65 'Operators' refers to the individuals or groups who engage in efforts to take advantage of computer vulnerabilities for either criminal or state-supported reasons. The term stands in contrast to 'attackers'; the latter term has fallen out of popular use for being overly militant.

66 See, for example: Crowdstrike. (2019). "Huge Fan of Your Work: How TURBINE PANDA and China's Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet," Crowdstrike; Nicholas Eftimi-ades. (2018). "Uncovering Chinese Espionage in the US," *The Diplomat.* Available at: https://thediplomat.com/2018/11/uncovering-chinese-espionage-in-the-us/; Office of Public Affairs. (2018). "Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies," *Department of Justice.* Available at: https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading.

67 Jeff Gray. (2011). "Hackers linked to China sought Potash deal details: consultant," *Globe and Mail.* Available at: https://www.theglobeandmail.com/technology/tech-news/hackers-linked-to-china-sought-potash-deal-details-consultant/article534297/.

68 Allegations in Canadian and international media suggest that Nortel, a Canadian telecommunications

Huawei to benefit from such campaigns is real in light of China's aggressive efforts to achieve equivalence and superiority in key industries, including telecommunications, by obtaining information to assist indigenous Chinese companies' own research and development activities.

Huawei's development of a large intellectual portfolio combined with American-led national security concerns has led Huawei to offer to license, in its entirely, its 5G-related intellectual property, so other nation-state actors or corporate researchers can evaluate the security of the company's products and produce the equipment themselves.[69] No Internet service or telecommunications provider in Canada has, at the time of writing, taken Huawei up on this offer, nor have any in the United States. It is possible that, to some extent, fair licensing may reduce some of the potential for Huawei—or, through soft power, the Chinese government—to unduly inhibit competitors from providing competitive 5G networking equipment.

However, even with a full licence, the national security concerns associated with evaluating patches and updates (discussed in more depth in section 6) may continue. Furthermore, licensing would not necessarily defray concerns of supporting Huawei's potentially illegitimate acquisition or use of other companies' intellectual property in its networking equipment. Finally, even with licences in hand, competing companies would still need to actually manufacture telecommunications equipment, and neither the United States or Canada possess a competitor to Huawei, thus inhibiting either government from benefiting from any licensing agreement.

4.2 - Mitigations

The intellectual property challenges linked with 5G are extensive, especially as they pertain to potentially improper activities undertaken by private companies along with espionage activities that may be conducted by state-associated operators. A set of discrete policies should be adopted that have the effect responding to 5G-related concerns while, at the same time, establishing a basis upon which the Government of Canada can build policies to address intellectual property theft and industrial espionage activities writ large.

company, suffered extensive data exfiltration and that the operators were located in China. While a number of former Nortel and Government of Canada employees have stated that Huawei benefitted from such espionage operations, there remains no open-source evidence to support such allegations. As an example of these kinds of allegations, see: Natalie Obiko Pearson. (2020). "Did a Chinese Hack Kill Canada's Greatest Tech Company?" *Bloomberg Businessweek.* Available at: https://www.bloomberg.com/news/features/2020-07-01/did-china-steal-canada-s-edge-in-5g-from-nortel.

69 Sijia Jiang (2019). "Huawei CEO says willing to license 5G tech to U.S. firm," *Reuters.* Available at: https://www.reuters.com/article/usa-china-huawei-tech/huawei-ceo-says-willing-to-license-5g-tech-to-u-s-firm-idUSB9N26700A.

First, Canada needs a comprehensive national approach to addressing foreign corporate espionage. At a high level, this approach should include better incentives for companies to report or share information; paths to international sanctions and domestic lawsuits; some reputation-shielding for implicated companies; and enhanced cooperation with foreign allies to punish state-facilitated or -enjoined espionage operations. More specifically, this approach could begin with Canada working more actively with other governments to encourage companies to report the suspected theft of intellectual property with the aim of advancing suspicions to investigations and, potentially, litigation. Canadian companies are often currently disincentivized from reporting IP theft: start-ups, on the basis that if they lose control of their IP, their valuations may suffer; and mid- and large-sized companies on the basis that lodging complaints could inhibit their ability to sell products to countries such as China. Additionally, companies may not believe that the government is likely to be helpful in cases of IP theft.[70] Should the government encourage such reporting, it should also explain the utility of such activities and not just take information in without meaningfully acting on it; such actions should be communicated to companies to encourage additional reporting. Efforts to encourage reporting and to act on provided information should be part of a broad strategy, as opposed to singling out any given company, and the efforts could be developed in such a way as to enable appropriate transnational sanctioning processes.

Second, Canada could increase its investment in Huawei's telecommunications competitors. At the moment, there are only two key competitors to Huawei—Nokia and Ericsson—and ensuring diversity in the market will prevent any single provider from gaining a monopoly in a market. At the same time, such investment could also enable Huawei's competitors to engage in contemporary and next-generation research and development. In January 2019, Canada allocated approximately $40 million (CAD) to Nokia to encourage the company to invest in research and development activities in Canada.[71] The goal of continuing such investments—perhaps in partnership with Canadian universities—would be to enhance Nokia and Ericsson's research capabilities surrounding 5G, with the ultimate aim of diversifying the number of companies that can produce high-quality and comprehensive 5G equipment—from the edges, to the core, and to critical elements of handset and end-point devices.

Third, the Government of Canada has provided private briefings to universities' employees about the national security concerns that are associated with research activities linked to Huawei, but it has failed to make public the specific concerns or proposed methods

70 The author thanks a range of corporate executives in Canada and the United States who, over the course of writing this report, anonymously spoke to him about the issues linked with reporting hacking to government authorities.

71 Andy Blatchford. (2019). "Huawei rival Nokia strikes $40-million research deal with Ottawa on 5G technology," *Financial Post.* Available at: https://business.financialpost.com/telecom/huawei-rival-nokia-strikes-40-million-research-deal-with-ottawa-on-5g-technology.

of mitigating risks. Underlying briefing materials should be made public as opposed to being kept cloistered within elite circles, and perhaps be routinely updated with information that lets universities develop plans to mitigate risks. In the face of distrust toward intelligence and security services after leaks about their activities and scathing judicial findings,[72] such transparency on the government's side could also serve to partially repair these agencies' credibility. Universities and their researchers could then develop and implement appropriate policies based on information presented by the government, perhaps paralleling or supplementing the resources that are provided by the Association of American Universities.[73] If the government is more generally concerned with universities receiving research funding from non-domestic companies, it should consider substantially increasing the funding allocated to basic and applied research that is undertaken by Canadian universities, and it should target the funds toward strategically identified sectors.

Finally, the Government of Canada could more prominently engage with the standards bodies, such as 3GPP, that are developing 5G standards. Currently, Canada, along with its allies, have been "woefully absent and need to make participation a priority".[74] Engagement may involve both the development of standards and participating with international fora to work toward mandating 5G security elements in 5G networks. At the time of writing, such security elements tend to be optional elements of the current 3GPP 5G standards. Domestically, the government could compel Canadian telecommunications companies to enable security elements in 5G or, alternatively, it could impose market penalties on companies that decline to enable such elements (e.g., held liable for damages or data exfiltrations where networks have not fully enabled 5G security elements). Should these approaches be found still lacking, the government could mandate baseline security standards that were vendor agnostic and that all Canadian carriers (and their vendors) were required to meet as a condition of providing 5G service in Canada. The government could also work to find ways, such as providing tax rebates

72 Phoenix Strategic Perspectives, Inc. (2020). "Attitudes towards the Communications Security Establishment — Tracking Study (Final Report)," *Government of Canada.* Available at: http://publications.gc.ca/collections/collection_2020/cstc-csec/D96-16-2020-eng.pdf, p. 13; Justin Ling. (2020). "Systemic shortcomings," *The Canadian Bar Association—National Magazine.* Available at: https://www.nationalmagazine.ca/en-ca/articles/law/hot-topics-in-law/2020/systemic-shortcomings.

73 Association of American Universities. (2020). "Science and Security Resources (June 2020)," *AAU.* Available at: https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/Science-and-Security-Resource-Document.pdf.

74 Alan Weissberger. (2020). "Strategy Analytics: Huawei 1st among top 5 contributors to 3GPP 5G specs," *IEEE COMSEC Technology Blog.* Available at: https://techblog.comsoc.org/2020/03/17/strategy-analytics-huawei-1st-among-top-5-contributors-to-3gpp-5g-specs/; see also: Mike Rogers. (2020). "The right frame of reference for 5G," *The Hill.* Available at: https://thehill.com/opinion/technology/487437-the-right-frame-of-reference-for-5g.

to organizations or individuals that become involved in such processes, of encouraging Canadian businesses and experts to participate in telecommunications standards setting. In the case of Canadian non-profit organizations and charities, the government could facilitate their inclusion by providing funds for registration fees, travel costs, and other expenses either directly from government departments or through vehicles such as the International Development Research Centre. In addition to telecommunications standards, the government should also prioritize encouraging individuals and organizations to take leadership roles in adjacent standards and norms-setting processes, such as those to promulgate the availability of strong encryption and to ensure the integrity of telecommunications systems and critical infrastructure.

Moving forward, with the 6G working groups already having begun their work, the Canadian government should actively encourage Canadian businesses and experts to participate in these working groups to, at least in part, ensure that security and privacy properties are aggressively baked into 6G standards as defaults. Furthermore, the government should carefully assess the efforts being undertaken at the International Telecommunications Union (ITU) to advance New IP, a protocol ostensibly intended to enable low latency Internet of Things functionalities that may maintain connectivity using 5G, but which may also enable heightened surveillance and control of data within national borders. The government should actively work to include Canadian experts in assessments of the propriety of New IP or to enable next-generation compute capabilities and functionalities that accord with Canadian principles and values.[75]

75 For more on New IP, see: Anna Gross and Madhumita Murgia (2020). "China and Huawei propose reinvention of the internet," *Financial Times.* Available at: https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2; Iain Morris. (2020). "Non-IP squares up to New IP in battle for Internet's future," *Light Reading.* Available at: https://www.lightreading.com/5g/non-ip-squares-up-to-new-ip-in-battle-for-internets-future/d/d-id/758771; Zhe Chen; Chang Wang; Guanwen Li; Zhe Lou; Sheng Jiang; and Alex Galis. (2020). "New IP Framework and Protocol for Future Applications." *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium,* Budapest, Hungary, 2020, pp. 1-5. Available at: http://prod-upp-image-read.ft.com/e8dd8c46-70e6-11ea-95fe-fcd274e920ca; Unknown Authors (Huawei Technologies Co., Ltd, P.R. China, China Mobile, China Unicom, and CAICT). (2019). "New IP, Shaping Future Network": Propose to initiative discussion of strategy transformation for ITU-T," *International Telecommunications Union.* Available at: http://prod-upp-image-read.ft.com/ec34d7aa-70e6-11ea-95fe-fcd274e920ca.

5. Monopoly and Trade Concerns

The success of Huawei's commercial operations raises monopoly and quasi-monopoly related concerns, for instance, about the implications of a single company becoming dominant within a critical telecommunications infrastructure. Linked with this possibility are trade concerns, such as the ways in which the Chinese government could exert influence to encourage countries that depend on Huawei equipment to develop China-friendly policies, that are formally separate from Huawei's own successes. After outlining these concerns, this section concludes with mitigations to address the aforementioned existent or prospective policy problems.

5.1 - Overview of Issues

Huawei's growth has partially depended on support from the Chinese government. The company's founder has stated that, "[i]f there had been no government policy to protect [nationally owned companies], Huawei would no longer exist."[76] More broadly, support from the Chinese government has included encouragement for domestic companies to purchase Huawei products,[77] the provision of state subsidies,[78] and credit extensions from the China Development Bank.[79] The government's strong support for indigenous technology companies has meant that Huawei—and other Chinese firms—enjoys a near-guaranteed, ongoing, domestic revenue stream, in contrast to their international competitors.

Huawei's impressive domestic growth is coupled with its rapid adoption into telecommunications networks around the world. Such international success has been predicated on the company's production of—depending on the source—good enough or truly excellent equipment, combined with a comparatively lower cost to purchase and operate the equipment versus that of its competitors, as well as assistance from Huawei engineers to install the equipment.[80] Each of these elements, on their own, serves as an incentive for companies to acquire and operate Huawei equipment. They are compounded

---

76 Alberto F. De Toni. (2011). International Operations Management, Lessons in Global Business. London: Routledge, pp 128. Citing Xiao, 2002, p. 127.

77 Brian Low. (2007). "Huawei Technologies Corporation: from local dominance to global challenge?" *Journal of Business & Industrial Marketing* 22(2), pp. 138-144.

78 Ryan Mcmorrow. (2019). "Huawei a key beneficiary of China subsidies that US wants ended," *Phys.org.* Available at: https://phys.org/news/2019-05-huawei-key-beneficiary-china-subsidies.html.

79 Doug Palmer. (2011). "Huawei rejects Eximbank chief's China aid claim," *Reuters.* Available at: https://www.reuters.com/article/us-usa-china-huawei-idUSTRE75F71220110616.

80 Drew FitzGerald and Stu Woo. (2018). "In U.S. Brawl With Huawei, Rural Cable Firms Are an Unlikely Loser," *Wall Street Journal.* Available at: https://www.wsj.com/articles/caught-between-two-superpowers-the-small-town-cable-guy-1522152000.

by Huawei's access to $100 billion (USD) in low-cost loans from state-backed banks that let foreign companies acquire Huawei's products at lower short- and long-term capital costs. The European Union[81] and Indian government[82] have both found that Huawei has violated anti-dumping guidelines, with the effect of impeding the competitiveness of EU and Indian companies. These loans and Huawei's other business operations may have enabled Huawei to unfairly extend its market share.

The means by which Huawei has grown as a company are not, on their own, inherently monopolistic. The company's increasing dominance could, however, enable Huawei to integrate capabilities into its 5G technologies that disadvantage their competitors. In particular, given Huawei's capability to produce all elements of a mobile telecommunications network, Huawei could integrate features in their end-point, radio, and core networking components that work in coordination with one another in excess of 5G standards. Such developments could encourage other 5G vendors to design their hardware and software to accommodate or make use of unique Huawei related features, or such integration may mean that Huawei equipment has significant benefits when used together in ways that competitors cannot match. Alternately, Huawei 5G equipment could be designed to impede telecommunications companies from easily adopting competitors' technologies for 6G, paralleling the design decisions that have gone into some of Huawei's 4G networking equipment.[83]

Information Box 3: Sole Vendor Infrastructures Increase Risks

In addition to distorting markets through loans and unique dependencies, there is a risk that Canadian telecommunications networks could experience heightened security threats if Huawei products come to dominate them. Such risks are not due to Huawei, per se, but to a more general lack of technological diversification. The security-related importance of diversification in the 5G stack was communicated by Scott Jones, Deputy Chief of Information Technology Security with the CSE before the House of Commons Standing Committee on Public Safety and National Security. Specifically, he said that,

81 Charlie Osborne. (2013). "EU: Huawei, ZTE 'dump' products in European markets," *ZDNet.* Available at: https://www.zdnet.com/article/eu-huawei-zte-dump-products-in-european-markets/.

82 IANS. (2016). "Huawei, ZTE telecom equipments face anti-dumping duty in India," *Telecomlead.* Available at: https://www.telecomlead.com/telecom-equipment/huawei-zte-telecom-equipments-face-anti-dumping-duty-india-68548.

83 The sticky nature of Huawei 4G networking equipment is discussed by Paul Triolo, though he also discussed how OpenRAN—a vendor-neutral disaggregation of hardware and software for 2G, 3G, and 4G networks—could undue this stickiness while recognizing that it will take between five and ten years before OpenRAN becomes a broadly viable option. For more, see: Anja Manuel and Paul Triolo. (2020). "Navigating China's Technological Rise: Critical Technology Regulation and its Industry Impact," *National Committee on U.S.-China Relations*. Available at: https://www.ncuscr.org/technology-regulation-industry-impact.

> **"…you don't want one vendor and only one vendor. That makes you vulnerable across your entire spectrum and across all of your telecommunications companies to the exact same vulnerability. You want to build in different vendors … That bakes in a large amount of security just because you can't easily traverse up and down the so-called telecommunications stack. That's one of the key elements for 5G."[84]**

For clarity, Huawei may achieve dominance in national telecommunications ecosystems if publicly or privately traded companies make investments that focus on shorter-term corporate returns rather than on longer-term implications of functional monocultures, where one vulnerability is widely shared throughout an industry. Moreover, capital investments are zero-sum, so acquiring Huawei equipment means that their competitors' products are not acquired, which could have the longer-term effect of enabling Huawei to invest more extensively in research and development than its competitors; thus, over time, their competitors potentially will have less robust products than Huawei. The outcomes of this feedback loop could be to create a very long-term strategic advantage for Huawei as its competitors become less able to offer equivalent products while simultaneously (and incidentally) generating a vendor monoculture.

As Huawei develops next-generation telecommunications equipment systems and products, the Chinese government could act to adjust either interest rates that are attached to Huawei equipment loans, the length of loan terms, or the availability of state-backed loans. Countries that adopt more China-friendly policies might see their firms receive preferential interest rates or term lengths compared to firms operating in jurisdictions that have less China-friendly policies. Such preferential practices could prospectively be used as elements of a broader foreign policy aimed at encouraging nations to modify their policies with regard to China and would complement the Chinese government's aggressive uses of trade bans to encourage the adoption of China-friendly policies, practices, or decisions.[85] Other risks might include the Chinese government's establishment of trade policies that make it challenging for Huawei to sell next-generation products to companies operating in countries that have adopted policies the Chinese government disapproves of. Such actions could hinder countries from acquiring next-generation technologies that

84 House of Commons Standing Committee on Public Safety and National Security, Evidence (Scott Jones, Deputy Chief, Information Technology Security, Communications Security Establishment), 42nd Parliament, 1st Session, 20 September 2018. For more, see: Sarah Lemelin-Bellerose. (2020). "5G Technology: Opportunities, Challenges and Risks," *Library of Parliament.* Available at: https://hillnotes.ca/2020/02/13/5g-technology-opportunities-challenges-and-risks/

85 Mark Lewis. (2011). "Norway's salmon rot as China takes revenge for dissident's Nobel Prize," *Independent.* (October 6, 2011). Available at: https://www.independent.co.uk/news/world/europe/norways-salmon-rot-as-china-takes-revenge-for-dissidents-nobel-prize-2366167.html; Canadian Press. (2019). "China ratchets up pressure on Canada by suspending another canola exporter," *CTV News* (March 27, 2019). Available at: https://www.ctvnews.ca/business/china-ratchets-up-pressure-on-canada-by-suspending-another-canola-exporter-1.4353805.

are compatible with previously installed Huawei equipment or even to maintain existing networks with the potential effect of impeding domestic telecommunications-driven economic innovation and development.

5.2 - Mitigations

The Canadian government could take up trade-related concerns linked to suspicions that Huawei is unduly benefiting from the Chinese government's assistance with international trade bodies such as the WTO. Some topics that might be raised include unfairly establishing protected domestic markets, providing undue advantage to domestic companies, or (in a future situation) using state-backed loans to unduly reward countries that adopt China-friendly policies. In addition to these international levers, Canada could use legal levers included in existing, or to be negotiated, bilateral or multilateral trade agreements.

The government—in tandem, perhaps, with private companies—could monitor companies' development of 5G-based technologies to assess whether any were specifically developing their 5G networking systems to enable vendor lock-in; thereby, detrimentally affecting the ability of telecommunications providers to adopt competitors' equipment in either stand-alone 5G networks or in next-generation 6G networks. Alternatively, some degree of lock-in might be permissible; the government could establish limits on how much any single vendor's equipment can suffuse a telecommunications network so as to reduce risks linked with comprehensive network lock-ins.

Finally, Canada could work with countries with complementary democratic traditions to encourage the adoption of products sold by Huawei's competitors in an effort to mitigate the risks linked to vendor monoculture. Specific mitigations might involve compelling telecommunications companies to diversify their equipment vendors, where any given vendor can compose only a certain percentage of a country's overall telecommunications infrastructure.[86] Diversification could be aimed at preventing Huawei, or any other company, from incidentally generating a 5G monoculture by ensuring competition between companies to prevent excessive rent-seeking behaviour, while better enabling companies to invest in next-generation technologies for later 5G innovations, 6G development, and so forth.

86 This is one of the requirements that had been established, in part, by the UK in its earlier decision to permit a limited quantity of Huawei equipment into its 5G telecommunications networks. For more, see: Ian Levy. (2020). "The future of telecoms in the UK," *National Cyber Security Centre.* Available at: https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk.

6. Technical Security Concerns

Members of the Five Eyes intelligence and security alliance have routinely raised technical security concerns associated with Huawei products and the company itself. This section differentiates between incidental and compelled technical vulnerabilities that are associated with Huawei's products, the utility of such vulnerabilities, and possible means of mitigating their impacts. To be clear, many of these risks are speculative insofar as there is limited public domain information that indicates that Chinese operators have compelled the insertion of any specific technical deficiencies in Huawei's telecommunications equipment.

6.1 - Technical Vulnerabilities

Technical vulnerabilities are deficits within a technical product that could be deliberately exploited to cause the product to operate in a way contrary to its owners' or users' preferences or desires. Vulnerabilities may constitute a kind of normal accident on the basis that very complicated systems invariably generate accidents (or vulnerabilities) due to their complexity.[87] Alternatively, vulnerabilities can be deliberately designed into products to facilitate law enforcement surveillance (e.g., lawful interception interfaces) or to enable foreign intelligence operations (e.g., espionage, disruption, or computer network attack).

6.1.1 - Incidental Technical Vulnerabilities

The United Kingdom's Huawei Cyber Security Evaluation Centre (HCSEC) has found a litany of technical deficits in the Huawei equipment it has reviewed. These deficiencies were "a particular concern" because, "[i]f an attacker has knowledge of these vulnerabilities and sufficient access to exploit them, they may be able to affect the creation of the network, in some cases causing it to cease operating correctly. Other impacts could include being able to access user traffic or reconfiguration of the network elements." These risks were being managed by UK telecommunications companies and the NCSC did not, "believe that the defects identified [were] the result of Chinese state interference."[88] Nonetheless, the technical director for NCSC, Ian Levy, stated in 2019 that the, "security of Huawei is like nothing else - it's engineering like it's back in the year 2000 - it's very, very shoddy."[89]

---

87 Perrow, Charles. (2011). *Normal Accidents: Living with High Risk Technologies.* Princeton University Press; Thomas Dullien/"Halvar Flake" (Google Project Zero). (2018). "Security, Moore's Law, and the Anomaly of Cheap Complexity," Video Presentation, CyCon, Tallinn, Estonia, 1 June 2018. Available at: https://www.err.ee/836236/video-google-0-projekti-tarkvarainseneri-ettekanne-cyconil.

88 Huawei Cyber Security Evaluation Centre Oversight Board. (2019). "Annual Report 2019," *Huawei Cyber Security Evaluation Centre.* Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

89 Leo Kelion. (2019). "Huawei's 'shoddy' work prompts talk of a Westminister ban." *BBC News*. Available at: https://www.bbc.com/news/technology-47830056.

Information Box 4: Subset of Known Incidental Vulnerabilities in Huawei Equipment

The United Kingdom's Huawei Cyber Security Evaluation Center's (HCSEC) 2019 annual report raised a number of deficiencies with Huawei equipment, such as:

- an inability to confirm that the source code examined by the Centre was "precisely that used to build the binaries running in the UK networks"
- an inability to be confident that Huawei equipment was "similarly secure" because vulnerabilities discovered in one build may not be remediated in another, similar, piece of equipment
- a poor configuration management protocol; without good protocol management, "there can be no end-to-end integrity in the products as delivered by Huawei"
- the company's use of "an old and soon-to-be out of mainstream support" version of an operating system had serious security deficits, to the point that the National Cyber Security Centre (NCSC), "believes there is currently no credible plan to reduce the risk in the UK of the use of this real time operating system" and that even moving to the operating system being developed by Huawei, "may not improve the situation long-term"
- flaws in the ways Huawei managed software component lifecycle management that required significant remediation of the company's existing codebase as well as the processes associated with lifecycle management more generally
- concerns that, "Huawei's software engineering and cyber security competence and associated processes" were failing to "improve sufficiently"
- an uncertainty that despite Huawei's expressed an intent to invest $2 billion over five years to remedy the defects that were found in the company's engineering processes, "it was not possible to offer any degree of confidence that the identified problems can be addressed by Huawei" serious concerns because HCSEC continued to find, "serious vulnerabilities in Huawei products…Several hundred vulnerabilities and issues were reported to UK operators to inform their risk management and remediation in 2018. Some vulnerabilities identified in previous versions of products continue[d] to exist". Of note, "[t]he character of vulnerabilities [had] not changed significantly between years, with many vulnerabilities being of high impact (equivalently, a high base CVSS score and relevant operational context), including unprotected stack overflows in publicly accessible protocols, protocol robustness errors leading to denial of service, logic errors, cryptographic weaknesses, default credentials and many other basic vulnerability types."

Supplementing the HCSEC's report, in early 2020, the United States publicly alleged to its allies that the lawful interception interfaces integrated into Huawei equipment could be secretly and remotely activated without carriers being aware of the activation.[90] It is unclear, based on open-source information, whether such activations (if they have actually taken place) were the result of vulnerabilities having been deliberately designed into the equipment's lawful interception interfaces, the result of Huawei's deficient engineering security practices, or another factor altogether. (Of note, lawful interception interfaces—functionally backdoors in routing equipment that are mandated by lawful access legislation in Europe and the Americas—for a range of Western vendors have, historically, also been repeatedly proven to be insecure.[91]) Finally, public reporting has showcased that some Huawei products have included remote administration systems (often referred to as 'backdoors' in the media)[92] that were inadequately secured. Some products also have included functionality that enabled remote administrators to tamper with logs to mask the activities that they had conducted.[93]

The aforementioned ranges of vulnerabilities have been found in switches, routers, and mobile networking equipment; however, none of these assessments were of Huawei's 5G equipment. While the HCSEC identified hundreds of issues with Huawei equipment

90 Bokan Pancevski. (2020). "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *The Wall Street Journal.* Available at: https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

91 Susan Landau. (2013). "The Large Immortal Machine and the Ticking Time Bomb," *Journal on Telecommunications and High Technology Law* 11(1); Tom Cross. (2010). "Exploiting Lawful Intercept to Wiretap the Internet," Blackhat DC, Washington, DC. Available at: https://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-LawfulI-Intercept-wp.pdf; Johannes Greil, Stefan Viehböck. (2014). "Root Backdoor & Unauthenticated access to voice recordings," *SEC consult Vulnerability Lab.* Available at: https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20140528-0_NICE_Recording_eXpress_Multiple_critical_vulnerabilities_v10.txt; Vassilis Prevelakis and Diomidis Spinellis. (2007). "The Athens Affair," *IEEE Spectrum.* Available at: http://spectrum.ieee.org/telecom/security/the-athens-affair; Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. (2014). "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping the Internet," Northwestern Journal of Technology and Intellectual Property 12(1).

92 Daniele Lepido. (2019). "Vodafone Found Hidden Backdoors in Huawei Equipment," *Bloomberg*. Available at: https://www.bloomberg.com/news/articles/2019-04-30/vodafone-found-hidden-backdoors-in-huawei-equipment.

93 Robert Graham. (2020). "Huawei backdoors explanation, explained," *Errata Security.* Available at: https://blog.erratasec.com/2020/03/huawei-backdoors-explanation-explained.html. Specifically, Graham writes: "At the same time, I also know that Huawei's maintenance/service abilities have been used for intelligence. Several years ago there was an international incident. My company happened to be doing work with the local mobile company at the time. We watched as a Huawei service engineer logged in using their normal service credentials and queried the VLR databases for all the mobile devices connected to the cell towers nearest the incident in the time in question. After they executed the query, they erased the evidence from the log files." Similar issues with auditing were previously found by Tom Cross in his assessment of lawful interception systems See: Tom Cross. (2010). "Exploiting Lawful Intercept to Wiretap the Internet," Blackhat DC, Washington, DC. Available at: https://www.blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-LawfulI-Intercept-wp.pdf.

that seem linked to the company's security culture, there plausibly remain many more vulnerabilities that have not been adequately identified and publicly reported.

Incidental technical vulnerabilities in Huawei equipment could potentially be brought to Chinese operators' attention before they are found in the course of UK technical assessments of Huawei equipment. This early revelation could happen as a result of agreements between Huawei and Chinese government institutions and have the effect of these vulnerabilities being used as bugdoors by Chinese operators. In effect, knowledge of vulnerabilities, especially when or if combined with a dictate to not patch any given subset of them, could potentially enable state-affiliated operators to undertake remote or local intelligence operations that rely on taking advantage of bugdoors.[94] Any discovery of a bugdoor could subsequently be blamed on Huawei's security culture, rather than as a result of an intervention by the Chinese government upon the private company.

In short: the assessments conducted by the HCSEC uncovered extensive vulnerabilities in Huawei equipment that operators might have taken advantage of. They also suggest that there will be a range of additional (and presently unknown) vulnerabilities that operators could take advantage of. Moreover, Huawei has not developed a culture that ensures that vulnerabilities are comprehensively patched across their product lines; discovering and patching one networking appliance is no guarantee that similar patches will be deployed across the company's product lines.[95] The HCSEC assessments conclude that a culture of insecurity will persist into the future, and thus it should be presumed to also apply to the company's 5G equipment. Huawei's historical failures to patch their products have been ascribed to its existing culture of (in)security, but they could also follow from Chinese government compulsions to leave certain vulnerabilities in place, so state-affiliated operators could take advantage of such bugdoors.

6.1.2 - State-Compelled Technical Vulnerabilities

It is a quip within the intelligence community that, "we have never found anything that the adversary has successfully hidden." Huawei might be compelled to modify its telecommunications products after receiving an order from Chinese officials pursuant

94 In addition to actual vulnerabilities, routing equipment can sometimes manifest what is best defined as weird, or unintended, behaviours that can be exploited by knowledgeable actors for cyber-related activities. As an example, the United States' National Security Agency took advantage of weird behaviours to secretly exfiltrate data from Yemennet telecommunications networks; this behaviour arose from the way in which a pair of networking appliances worked in tandem with one another. Deep technical knowledge from the vendor that explains how appliances operate could provide Chinese intelligence and security services with significant—and very hard to detect—advantages. For more, see: National Security Agency. (2007). "Network Shaping 101," National Security Agency. Available at: https://assets.documentcloud.org/documents/2919677/Network-Shaping-101.pdf.

95 Such technical deficiencies are made worse by the often-slow rate at which telecommunications providers deploy security patches to their core networking infrastructure and associated radio access networks.

to Chinese national security law.[96] Commentators have written that the National Intelligence Law creates, "affirmative legal responsibilities for Chinese and, in some cases, foreign citizens, companies, or organizations operating in China to provide access, cooperation, or support for Beijing's intelligence-gathering activities" whereas the earlier State Security Law enabled the Chinese government to "compel Chinese companies and Chinese citizens working in the United States to assist the Chinese government with the broadly defined mission of "safeguarding State security."[97] Assessments of the definitional relationship between "safeguard state security," and "external interference" to state security and the ability to broadly mandate Chinese businesses or citizens to assist the Chinese government form the basis for arguments that the Chinese government might compel companies or employees to modify telecommunications equipment or associated software to benefit the Chinese government's cybersecurity, intelligence, or counterespionage operations.

Members of the Five Eyes countries have been warned of the risks associated with Chinese government interference with China-based supply chains[98] since at least 2009.[99] Some classified warnings from the American national security establishment have been shared with Canada and the other Five Eyes partners. One warning advised the intelligence community to look at the Chinese supply chain, writ large, on the basis of, "[t]he deep influence of the Chinese government on their electronics manufacturers, the increasing complexity and sophistication of these products, and their pervasive presence

96 Specific concerns have been raised by critical commentators about the National Intelligence Law, Counterespionage Law, and the Cybersecurity Law. See: Murray Scot Tanner. (2017). "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*. Available at: https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; Jason Silver. (2015). "China's Asymmetric Intelligence Advantage: The State Security Law," Orbis 59(3); Valentin Weber. (2019). "Finding a European response to Huawei's 5G ambitions," *Norwegian Institute of International Affairs.* Available at: https://pdfs.semanticscholar.org/d308/3c6dbb9c7b9234f836e27ee11713da3317e9.pdf. For an opposing view, see: Chen Jihon and Jianwei Fang. (2018). "Before the Federal Communications commission," *FCC.* Available at: https://thechinacollection.org/wp-content/uploads/2019/03/Huawei-Declaration.pdf.

97 Jason Silver. (2015). "China's Asymmetric Intelligence Advantage: The State Security Law," *Foreign Policy Research Institute.* For more, see: "China's intelligence law and the country's future intelligence competitions" in *Rethinking Security: China and the Age of Strategic Rivalry.* Canada. Available at: https://www.canada.ca/content/dam/csis-scrs/documents/publications/CSIS-Academic-Outreach-China-report-May-2018-en.pdf.

98 The National Institute of Standards and Technology has listed six types of cyber supply chain risks: insertion of counterfeits; unauthorized production of components; tampering with production parts and processes; theft of components; insertion of malicious hardware and software; and poor manufacturing and development practices that compromise quality. For more, see: Information Technology Laboratory / Computer Security Resources. (2020). "Cyber Supply Chain Risk Management," *NIST.* Available at: https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management.

99 Earlier work—dating back to 2005 and earlier—recognized the challenges and risks linked with offshoring sensitive electronics such as semiconductors. See: Clair Brown and Greg Linden. (2005). "Offshoring in the Semiconductor Industry: A Historical Perspective," Industry Studies Association Working Papers. Available at: http://isapapers.pitt.edu/58/1/2005-02_Brown.pdf.

in global communications networks increases the likelihood of the subtle compromise — perhaps a systemic but deniable compromise — of these products."[100] Concerns—though highly redacted or opaque—have also been raised by Canadian agencies about national security concerns associated with deploying Huawei equipment in Canadian companies' networks.[101]

Information Box 5: Targeting State-Compelled Vulnerabilities

There are at least three general classes of vulnerabilities that a state actor might compel a private telecommunications vendor to insert: those associated with hardware, with firmware, and with software.

Where a state compels the injections of a vulnerability, any efforts to do so throughout a vendor's products are comparatively more likely to be discovered in testing (and thus less effective) than those that have been selectively deployed against specific targets or infrastructure. Targeting capacity is enhanced by possessing intelligence about who is purchasing a product and where it might be deployed.

Companies that assist private telecommunications companies to develop, update, or maintain their networks may be of particular interest to a Chinese state intelligence and security agency. Huawei, with its knowledge of which company is receiving equipment or the company technicians who will help to install the equipment, could provide valuable targeting information to the Chinese government or state-affiliated operators.

Hardware vulnerabilities can involve modifications to the power systems, motherboards, memory, or other hardware components in telecommunications equipment. Hardware modifications can take place at their point of creation, in transit, or after they have reached where they are to be operated. In all such cases, adversaries may depend on human sources to perform the modifications. In Canada, the CSIS has warned that the Chinese government might compel persons in Canada to work to advance Chinese interests, with the CSIS director having said that, "[w]hile some nationals in Canada assist their governments willingly, many do so begrudgingly out of fear of state retribution upon

100 Office of the Director of National Intelligence. (2009). "National Intelligence Estimate: The Global Cyber Threat to the US Information Infrastructure," National Intelligence Council. Available at: https://assets.documentcloud.org/documents/5691428/National-Intelligence-Estimate-2009-Global-Cyber.pdf.

101 Communications Security Establishment Canada (CSE). (2012). "A-2012-00397: Briefing note to the DG Cyber: "NATO multinational cyber defence capability development - MOU," Government of Canada; Steve Chase. (2019). "Canadian intelligence agencies at odds over whether to ban Huawei from 5G networks: official," Globe and Mail. Available at: https://www.theglobeandmail.com/politics/article-canadian-intelligence-agencies-disagree-on-whether-to-ban-huawei-from/.

them or their families."[102] The warning from the CSIS, made in 2019, reaffirms a similar notice that was included in the 2009 National Intelligence Estimate from the Office of the Director of National Intelligence. That 2009 notice read that, "China's state-sponsored information operations capabilities will continue to grow. Chinese cyber efforts include *insider access, close access, remote access, and probably supply chain operations.*"[103] The threats posed by close-access operations undertaken by de facto agents of the Chinese government are not new but are, instead, persistent in nature.[104]

Whereas targeting hardware involves manipulating the physical characteristics of a piece of equipment, there are a pair of related code-based methods of manipulating telecommunications equipment worth noting. Specifically, states might undertake efforts to target firmware or software that is associated with equipment.

Firmware provides a low-level control of a specific device's hardware and receives commands passed to it from higher-level software.[105] Telecommunications equipment's firmware is rarely updated, which means that, "[a]ny compromises against the older versions have a 'forever day' aspect that means that they will remain useful for adversaries against systems that might be in use for many years."[106] It is entirely possible that firmware vulnerabilities may never be detected. Trammell Hudson, a security researcher who has previously identified significant BIOS vulnerabilities, has said that, "[i]t's very puzzling that we haven't seen evidence of more firmware attacks … Most every security conference debuts several new vulnerability proof-of-concepts, but … the only public disclosure of compromised firmware in the wild" emerged in 2015 when Kaspersky Labs identified hard drive firmware implants which were attributed to the NSA. Hudson's conclusion is that, "[e]ither as an industry we're not very good at detecting them, or these firmware attacks and hardware implants are only used in very tailored access

102 Douglas Quan. (2019). "'Significant and clear' threat: What Canada's spy chief says about China behind closed doors", *National Post.* Available at: https://nationalpost.com/news/canada/significant-and-clear-threat-what-canadas-spy-chief-says-about-china-behind-closed-doors.

103 Office of the Director of National Intelligence. (2009). "National Intelligence Estimate: The Global Cyber Threat to the US Information Infrastructure," National Intelligence Council. Available at: https://assets.documentcloud.org/documents/5691428/National-Intelligence-Estimate-2009-Global-Cyber.pdf. Emphasis not in original.

104 While there may be specific concerns that agents operating for China might modify Huawei equipment either during manufacture, delivery, or installation, it is worth recognizing that such concerns are not unique to 5G-based equipment. The same concern exists about any product manufactured in China, transited around the world, and ultimately installed in either Canadian telecommunications or other critical infrastructure environments.

105 In some cases, such as with relatively simple devices, the firmware may constitute the entirety of the software stack, such as with Internet of Things (IoT) devices like fridges, computer peripherals, etc.

106 Micah Lee and Henrik Moltke. (2019). "Everybody Does It: The Messy Truth About Infiltrating Computer Supply Chains," *The Intercept.* Available at: https://theintercept.com/2019/01/24/computer-supply-chain-attacks/.

operations."[107] Such operations are predominantly associated with well-resourced, state-backed operators.

Firmware modifications might be made during the manufacture or delivery of hardware, as well as potentially upon (or following) delivery vis-a-vis a remote access operation or, less likely, a close-access source operation. Given that Huawei equipment is made and delivered to clients out of China, it is perhaps most plausible that Chinese security and intelligence services would modify firmware before the product was delivered and target hardware after encouraging or pressuring Huawei to disclose where the equipment was destined, who planned to operate it, or its presumed future placement in a telecommunications company's network.[108] It is next likely that remote functionalities could be used to update firmware components. Least likely, though within the realm of possibility, is that close-access operations could be conducted, though such operations tend to have a high risk of discovery or exposure. The People's Liberation Army has undertaken active efforts to target firmware since at least 2012.[109]

Telecommunications routing equipment runs unique operating systems that are responsible for passing instructions to the equipment's firmware. Chinese state security or intelligence services could potentially compel Huawei to insert vulnerabilities into these operating systems or the software libraries that are integrated into their products. Such compulsions might target employees of Huawei without the knowledge of their managerial staff, might involve directing dual-hatted Huawei employees who are also government employees, or might entail compelling the company to modify the software. In all cases, the vulnerability might be presented not as a backdoor but as a method of facilitating lawful interception, a way to stop a device from transmitting certain kinds of malicious communications, or other functionalities that have ostensibly benign purposes but that could be manipulated by knowledgeable operators for less benign purposes.[110]

---

107 Micah Lee and Henrik Moltke. (2019). "Everybody Does It: The Messy Truth About Infiltrating Computer Supply Chains," The Intercept. Available at: https://theintercept.com/2019/01/24/computer- supply-chain-attacks/.

108 The practice of interdicting equipment before it is delivered has been a tactic adopted by Five Eyes Countries and their allies, and especially the United States. The NSA has worked to interdict equipment that was ultimately installed into the Syrian Telecommunications Establishment (amongst others), to the effect of gaining access to vast swathes of the country's telecommunications infrastructure, both wired and wireless. For more, see: Chief, Access and Target Development. (2010). "Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets," *SID Today.* Available at: https://github.com/nsa-observer/documents/blob/master/files/pdf/media-35669.pdf.

109 Unknown Author. (2012). "BIOS Threats," *Intellipedia.* Available at: https://assets.documentcloud.org/documents/5691425/Intellipedia-BIOS-Threats.pdf.

110 Even companies that employed individuals to create secure communications hardware have successfully convinced employees to overlook or ignore deliberate vulnerabilities in the sold products over the course of decades and where the products were used in national security communications; there is no self-evident reason why similar kinds of behaviours couldn't occur in other companies. See: Greg Miller. (2020). "The intelligence coup of the century," *Washington Post.* Available at: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.

6.1.3 - Potential Utility of Technical Vulnerabilities

Threats posed by potential technical vulnerabilities associated with Huawei 5G telecommunications equipment can broadly be captured under the Confidentiality, Integrity, and Availability (CIA) triad. Confidentiality refers to setting rules that limit unauthorized access to information; integrity refers to assurances that the information is trusted and authentic; and availability refers to the reliable access to the information by authorized persons. In each of the below cases, I discuss how either incidental or compelled vulnerabilities could be exploited to weaken or undermine one or more aspects of the CIA triad.

6.1.3.1 - Espionage

Operators might leverage vulnerabilities within 5G systems to compromise confidentiality. Espionage activities can involve an operator exfiltrating information from an information system, contrary to the controls that have been established by the owner or controller of the information system. If equipment is compromised by either local or remote tampering, data that is routed either through radio access networks or core networking systems could be rerouted to unauthorized locations. Rerouted information might include content, where data was unencrypted, or metadata, which will continue to tend to be unencrypted to some extent when using 5G networks. Exfiltration might include larger or smaller volumes of data, depending on what is targeted for collection, how the data is encrypted, and the means by which operators can transfer data to their own collection systems.

Information Box 6: Espionage Risks and Huawei 5G Equipment

Canadian organizations already have espionage-related concerns; they are targets now, and current espionage activities do not rely on vulnerabilities in any one company's software or hardware. Going forward, however, and should Huawei 5G equipment be widely integrated, there may be an enhanced risk that foreign operators with specific, unique knowledge of Huawei appliances or vulnerabilities in these appliances could take advantage of the equipment to further extend existing espionage activities.

Operators might also seek to compromise the logical separation(s) between virtualized elements of 5G networks. Much of the promise of 5G is premised on the idea that business groups will be better able to obtain access to networking capability to fulfill their business objectives.[111] As an example, networks could be configured to slice some of the available

111 For more, see: Peter Rost, Ignacio Berberana, Andreas Maeder, Henning Paul, Vinay Suryaprakash, Matthew Valenti, Dirk Wübben, Armin Dekorsy, and Gerhard Fettweis. (2015). "Benefits and Challenges of Virtualization in 5G Radio Access Networks," *IEEE Communications Magazine—Communications Standards Supplement* (December 2015); J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J.J. Ramos-Munoz,

networking capability to facilitate sensing of where different equipment on an advanced factory floor is located and enable rapid repurposing of the factory without needing to rewire the building.[112] In such a situation, espionage could be directed toward exfiltrating information about existing factory designs or configurations to inform China's targeted economic development sectors. Alternately, factory equipment that is being used to build products associated with national security-related products (e.g., munitions, advanced metallurgy, shipbuilding, etc) could be targeted to provide information about Canada's national defensive capabilities to the Chinese government. Similarly, should aspects of the 5G network be sliced to enable particular capabilities for government agencies, such as the military, compromising the virtualized elements might reveal activities or communications that are meant to be kept from unauthorized parties.[113]

6.1.3.2 - Disruption or Attack

Disruption activities negatively affect the integrity and availability of communications and sometimes affect their confidentiality. Disruption activities encompass events that seek, "to impact an organization's ability to produce and deliver a good/service, or to communicate with its target audience."[114] Disruptions can include modifying communications content or metadata or temporarily impeding communications functions; all such activities might be undertaken by compromising specific virtualized functions of a 5G system or by targeting the underlying hardware associated with facilitating communications.

Modifying communications could cause incorrect information to be communicated from the network to devices closer to the edge or, in contrast, could modify data that equipment near the edge of the network transmits to the core. Such an activity might include sending false data to manufacturing equipment such that the equipment fails to perform its tasks or, modifying data that such equipment sends to the network in such a way that the network cannot intake the data appropriately, and the network subsequently directs the equipment to take inappropriate actions. More broadly, by compromising the integrity of a communications network involved in big data collection, the subsequent

J. Lorca, and J. Folgueira. (2017). "Network Slicing for 5G with SDN/NFV: Concepts, Architectures and Challenges," *IEEE Communications Magazine*; Faqir Zarrar Yousaf, Michael Bredel, Sibylle Schaller, and Fabian Schneider. (2017). "NFV and SDN - Key Technology Enablers for 5G Networks," *IEEE Journal on Selected Areas in Communications* 35(11).

112 Stephanie Carvin. (2020). "Ep 118 What even is 5G anyway?" *Intrepid Podcast*. Available at: https://www.intrepidpodcast.com/podcast. The example of advanced factory capabilities was suggested by David Everinghan, Ericsson's VP and Chief Technology Officer.

113 Ellen Nakashima and Souad Mekhennet. (2019). "U.S. officials planning for a future in which Huawei has a major share of 5G global networks," *The Washington Post*. Available at: https://www.washingtonpost.com/world/national-security/us-officials-planning-for-a-future-in-which-huawei-has-a-major-share-of-5g-global-networks/2019/04/01/2bb60446-523c-11e9-a3f7-78b7525a8d5f_story.html.

114 Charles Harry. (2015). "A Framework for Categorizing Disruptive Cyber Activity and Assessing its Impact (Working Paper)," *Centre for International & Security Studies at Maryland (CISSM).* Available at: https://cissm.umd.edu/sites/default/files/2019-07/CategorizingDisruptiveCyberActivity%20-%20080615.pdf.

computations and decisions based on the data might be biased in ways that do not reflect the ground truth of the world that has been perceived by the sensors.

Should disruption activities affect the availability of networking resources, the activity could prevent the equipment from transmitting or processing communications data. The result might be that the devices to which the affected piece of telecommunications equipment was communicating—either elements of the telecommunications network itself, or devices on the edge of the network—would be unable to complete the tasks expected of them. A secondary consequence of a disruption activity of this type might be to affect the confidentiality of data. This consequence could arise should an affected networking system shift to using a less-secure means of communication or data processing as a result of the disruption. Indeed, should an adversarial operator know that a disruption might move communications or processing to a less-secure environment, the disruption itself might be motivated to compromise confidentiality so as to enable espionage.

Disruption activities might take place for obvious and extended periods of time or intermittently, thereby detrimentally affecting network operations in a targeted manner that causes network operators to expend significant resources to identify, trace, and mitigate the source(s) of the detrimental activity. Where they affect networks that enable Internet of Things connectivity—such as heating systems, sewage control, traffic lights, or elements of medical facilities—disruptions of the network could have significant secondary consequences. Where the disruption activities are meant to permanently disable networking functionality, they might be better understood as computer network attacks. The core differences between disruption and attack, under this framing, is the duration of the disruption and the operator's intent.

6.2 - Mitigations

There are numerous mitigation strategies that might address the potential for Huawei equipment to be exploited for espionage or disruption activities. Broadly, these strategies include: information assurance, security and foreign intelligence operations, network-based analytics and virtualization, vendor diversification, and broad use of end-to-end encryption. While many of these mitigations involve technical responses, in most cases, the issues are linked to broader social and political situations. As such, government-led mitigations should be conducted in accordance with guidance from other stakeholders, such as civil society that is external to government, foreign affairs officers, well-informed counsel, and private businesses that are responsible for operating Canadian networks.

6.2.1 - Information Assurance

Information assurance (IA) operations, "protect and defend information and systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

These measures include providing for restoration of systems by incorporating protection, detection, and reaction capabilities."[115] IA can involve a range of activities that are associated with the lifecycle of the equipment and information in question, and they may include conducting risk analyses that prioritize particular security goals, selecting security countermeasures based on cost-effectiveness and efficacy, tracing security measures over every stage of the equipment's lifecycle for consistency, and evaluating the assessments and mitigation processes for completeness.[116] In the case of Huawei equipment, the UK's HCSEC publishes information assurance assessments in public annual reports, blog postings by its director, and in advice provided to UK telecommunications companies.

In Canada, the Communications Security Establishment has assessed Huawei's telecommunications equipment as part of the Security Review Program since 2013. The Program has excluded designated equipment from sensitive areas of Canadian networks, imposed mandatory assurance testing on products before they are used in less sensitive areas of Canadian networks, and restricted managed services across Government of Canada networks and other critical Canadian networks.[117]

Mandatory testing, using the Common Criteria for Information Technology Security Evaluation ("Common Criteria"), is also conducted on products to assess the security of a range of information technology products used in Government of Canada networks and that are involved with the transmission, storage, or processing of sensitive information. Common Criteria testing is performed by independent labs that are accredited by the Government of Canada in tandem with testing performed by other countries and laboratories around the world. Some of Huawei's products have been assessed under the Common Criteria.[118] Of note, the Common Criteria assesses whether a product does what it says it will do and meets the claimed security functionality; the framework associated with these assessments, "focuses on the process rather than product…there is nothing in the protection profile that provides any confidence or assurance to the customer that [companies] have done a good job" in eliminating vulnerabilities.[119] It is

115 National Institute for Standards and Technology. (2017). "NIST Special Publication 800-12: An Introduction to Information Security," *NIST*. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf.

116 Yulia Cherdantseva and Jeremy Hilton. (2013). "A Reference Model of Information Assurance & Security," *IEEE proceedings of ARES 2013*, SecOnt workshop (2-6 September, 2013, Regensburg, Germany).

117 Canadian Centre for Cyber Security. (2018). "CSE's Security Review Program for 3G/4G/LTE in Canadian Telecommunications Networks," *Canadian Centre for Cyber Security.* Available at: https://cyber.gc.ca/en/news/cses-security-review-program-3g4glte-canadian-telecommunications-networks.

118 For a listing of Common Criteria products, see: https://www.commoncriteriaportal.org/products/.

119 William Jackson. (2007). "Under attack," *Government Computer News.* Available at: https://gcn.com/Articles/2007/08/10/Under-attack.aspx?Page=1.

only with higher-level evaluations that systems' computer code is evaluated or assessments conducted to reveal how products work in practice.

No assessment process is a panacea to security vulnerabilities. However, Tony Sager, a former employee of the National Security Agency who looked for vulnerabilities in products, has said that:

> I used to look at other peoples' software for a living and find zero-day bugs. What I realized was that our ability to find things as human beings with limited technology was never going to solve the problem. The deterrent effect that people believed someone was inspecting their software usually got more positive results than the actual looking. If they were going to make a mistake – deliberately or otherwise — they would have to work hard at it and if there was some method of transparency, *us finding the one or two and making a big deal of it when we did was often enough of a deterrent.*[120]

Extending and amplifying existing assessment of telecommunications equipment, through enhancing Canada's involvement with Common Criteria, making public the vulnerabilities that are detected in critical networking technologies, and ensuring that telecommunications companies and integrators are applying an assessment framework to confirm that their products are operating normally may mitigate some threats associated with efforts to interfere with critical Canadian telecommunications infrastructures. Beyond developing systems to detect if network appliances have been tampered with or modified such that they possess vulnerabilities that could be exploited by foreign operators, members of private industry and government alike should develop (and test) processes that enable networking elements or appliances to be deactivated with minimal disruption of communications and implement ways to remediate potentially compromised networking elements of appliances.

6.2.2 - Security and Foreign Intelligence Operations

The CSIS as well as the CSE may undertake operations that are designed to identify specific threats to Canada. Under their respective mandates, they can act to reduce threats to the security of Canada and, in the case of the CSE, can engage in active or defensive cyber activities to deter or stop operations that are detrimental to Canadian international affairs, defence, or security.

The CSIS principally uses human intelligence to collect security intelligence where there is a nexus to Canada. The Service may engage in operations designed to mitigate threats to the security of Canada that may arise from espionage or sabotage, foreign influenced activities that are detrimental to Canadian interests, activities that might be undertaken

120 Brian Krebs. (2018). "Supply Chain Security 101: An Expert's View," *Krebs On Security.* Available at: https://krebsonsecurity.com/2018/10/supply-chain-security-101-an-experts-view/. Emphasis not in original.

against persons or property to achieve political objectives, or any activities that aim to overthrow the constitutionally established system of government in Canada.[121] In the context of critical networking infrastructure, such as 5G appliances, the Service's mandate would enable it to use human sources within and outside of Canada to collect intelligence pertaining to whether, as an example, Huawei appliances were being modified to enable Chinese operators' activities. The Service might also collect information about Canada-based consular officials or undeclared intelligence officers who sought to facilitate or oversee either remote or close-access operations. Further, the Service's disruption capabilities might be exercised, following consultation with other agencies, to ward off threats toward Canadian 5G infrastructure where the threat has a nexus with regard to Canada. Notably, disruption operations may involve either physical or digital operations.[122]

Canada's foreign signals intelligence agency, the CSE, can undertake a range of operations intended to mitigate potential risks to critical Canadian telecommunications infrastructure. Four aspects of the agency's mandate are worth highlighting. First, pursuant to section 16 of the *CSE Act*, the agency can conduct foreign signals intelligence operations to collect information from or through the global information infrastructure so as to provide the Government of Canada with information that pertains to the government's intelligence priorities. Operations may include targeted or mass/bulk surveillance activities that aim to acquire intelligence about foreign individuals, states, organizations, or terrorist groups as they relate to international affairs, defence, or security.[123] The CSE can (and most likely does) target foreign telecommunications vendors, elements of foreign governments responsible for directing or receiving intelligence that is exfiltrated after compromising telecommunications networks, and organizations that might operate in the service of foreign governments to the detriment of Canadian foreign affairs, defence, or security. More specifically, such operations could include assessing whether foreign telecommunications vendors, including Huawei, are engaged in activities that run counter to Canadian interests as well as any potential actions taken by Chinese operators to exploit vulnerabilities in existent telecommunications infrastructures.

Second, the CSE can undertake activities pursuant to Section 17 of the *CSE Act*. Under this section, the CSE can acquire, use, and analyze information from the global information infrastructure and other sources to provide the advice, guidance, and services to protect the Government of Canada's electronic information and information infrastructures as

121 Canadian Security Intelligence Service Act, Section 2 ("threats to the security of Canada").

122 *Canadian Security Intelligence Act*, Section 21.1. For more on CSIS's threat disruption capabilities, see: Michael Nesbitt. (2019). "Bill C-59 and CSIS's 'New' Powers to Disrupt Terrorist Threats: Holding the Charter-Limiting Regime to (Constitutional) Account," *Alberta Law Revie*w 57(1). Available at: https://www.albertalawreview.com/index.php/ALR/article/view/2575.

123 *CSE Act*, section 2.

well as electronic information and information infrastructures explicitly designated as being of importance to the Government of Canada. The minister enjoys discretion to designate any non-government electronic information, infrastructure information, or class thereof as important and can bring it within the scope of the CSE's cybersecurity and information assurance mandate. Even after being identified as important, the CSE may only undertake activities under this Section to assist non-government organizations after those organizations have formally requested the CSE's assistance. Activities undertaken under this aspect of the CSE's mandate might include placing sensors or probes in private telecommunications providers' networks to detect known or suspicious networking events and advising how to mitigate those events or working with the permission of the network owner to terminate the events. Thus, the CSE could potentially work with telecommunications carriers to intercede in situations where 5G networking appliances were behaving in suspicious ways or being used to illicitly modify or exfiltrate data.

Third, the CSE could prospectively be involved in either defensive or active cyber operations to mitigate threats associated with Canada's 5G networking infrastructure. Defensive operations include activities designed "to help protect federal institutions' electronic information and information infrastructures" as well as other electronic information and information infrastructures that have been designated as being of importance to the Government of Canada.[124] Active cyber operations include activities designed "to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security".[125] Either class of these operations might be utilized to undertake activities meant to prevent operators from exploiting vulnerabilities in Huawei equipment, from undertaking remote access operations potentially designed to inject vulnerabilities in firmware or software, or otherwise carry out operations that rely on Huawei (or other vendors') equipment and that either endangers electronic information and information infrastructures of importance to the Government of Canada or that threatens Canada's international affairs, defence, or security.

Operations that either the CSIS or the CSE might undertake can increase the cost of secretly inserting or exploiting vulnerabilities in 5G networking appliances and, if acts that threaten the interest of Canada are detected, can potentially lead to actions being undertaken. Operations undertaken by these agencies cannot guarantee that vulnerabilities in next-generation 5G networking appliances are present or not, but they can, in tandem with other mitigation strategies, provide heightened assurance and assessment

124 *CSE Act*, section 18.

125 *CSE Act*, section 19.

of the security of the critical infrastructure and active measures where vulnerabilities are being exploited.[126]

6.2.3 Network Monitoring, Diversification, and Virtualization and Strong Encryption

Canadian telecommunications companies undertake a range of activities to detect abnormal networking events. Next-generation, artificial-intelligence-enhanced defensive tools could be leveraged to better identify suspicious data traffic or network events in current as well as 5G telecommunications systems.[127] The efficacy of such monitoring and tools, however, remains an understudied area in the context of nation-state or state-adjacent intelligence, espionage, or computer network attack operations. Companies and the Government of Canada could extend the ways in which they share indicators of compromise and threat signatures, such as through the Canadian Cyber Threat Exchange (CCTX), to better ensure that Canadian network providers can protect their systems and customers. As discussed in 6.2.2, Canadian telecommunications companies could also avail themselves of the defensive monitoring systems that are available through the CSE, under Section 17 of the *CSE Act.*[128]

The Canadian government could require Canadian telecommunications companies to integrate a diverse set of vendors into their networking infrastructures. The goal of such a policy would be to limit the specific harms that might be done should a particular vendor's equipment be compromised or otherwise configured to operate contrary to the interests of a telecommunications provider or its customers. Any and all appliances that are integrated into Canadian networks should have to have all of the security elements denoted in the 5G standards enabled. The Canadian Radio-television and Telecommunications Commission (CRTC) should be responsible for publicly assessing that such properties are, in fact, engaged.

---

126 There is, however, a risk that detected vulnerabilities may be retained by these agencies for their own operations. While the vulnerabilities might be known in such cases, the government agencies' knowledge of them would not necessarily translate into a more secure Canadian infrastructure. The infrastructure could still be exploited should the vulnerabilities not be publicly disclosed.

127 For more on this, see: Bruce Schneier. (2018). "Artificial Intelligence and the Attack/Defense Balance," *IEEE Security & Privacy* 16(2). Available at: https://ieeexplore.ieee.org/document/8328965.

128 For a discussion of the cybersecurity and information assurance elements of the CSE's mandate, see: Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson, and Ronald Deibert. (2017). "Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (An Act respecting national security matters), First Reading (December 18, 2017)," Citizen Lab & CIPPIC. Available at: https://citizenlab.ca/2017/12/citizen-lab-and-cippic-release-analysis-of-the-communications-security-establishment-act/. Note that since the legislation has been introduced, some minor changes have been made to the legislation.

Finally, the virtualization offered by 5G systems in combination with end-to-end encryption may mitigate some threats posed by compromised telecommunications equipment. While compromised equipment might be leveraged to breach the virtualized elements of a 5G network, virtualization could still potentially introduce an additional layer of friction for operators who attempt to access these elements. Ensuring the availability of strong encryption on end-point devices could also mitigate some risks associated with compromised networking equipment, insofar as encryption would provide confidentiality in the content of communications and integrity verification could confirm that received communications had not been modified or tampered with. Encryption does not, however, inherently resolve availability-related issues should networking equipment be disabled or prevented from transmitting communications.[129]

129 For more, see: Herb Lin. (2019). "Huawei and Managing 5G Risk," *Lawfare* (April 3, 2019). Available at: https://www.lawfareblog.com/huawei-and-managing-5g-risk.

7. Politics and China's Rule by Law

Huawei executives have asserted that they comply with domestic Canadian legislation and, thus, have not and will not undertake espionage or information operations on behalf of the Chinese government. Furthermore, Huawei's founder has asserted that Huawei will resist any efforts by the Chinese government to compel the insertion of vulnerabilities into the company's products. Experts, however, have routinely questioned the extent to which China complies with the rule of law and, thus, whether the protestations of Huawei executives are sufficient to satisfy concerns that the Chinese government could use national security law to compel Huawei to inject or retain vulnerabilities in networking appliances sold to Canadian telecommunications companies.

This section provides a broad overview of how Chinese law operates in practice, demonstrating that the assertions that have been made by Huawei executives do little to assuage concerns that the company could be compelled to modify its products to satisfy Chinese intelligence or national security laws. As such, Chinese law is unlikely to mitigate any prospective modification of Huawei equipment.

7.1 - China and Rule of/by Law

Since the late 1980s, the Chinese Communist Party has systematically worked to improve the state of its judiciary. These efforts have included improving the legal awareness and education of Chinese citizens,[130] professionalizing the judiciary post-2003,[131] and better enabling the judiciary to engage in cross-citation of cases through enhancements to information technologies.[132] Further, China has—within its own judicial architecture—

---

130 Susan H. Whiting. (2017). "Authoritarian "Rule of Law" and Regime Legitimacy," *Comparative Political Studies* 51(14): 1907-1940; Young Nam Cho. (2016). "China's "Rule of Law" Policy and Communist Party Reform," Asian Perspective 40: 675-697.

Of note, however, the popular legal education "has provided basic legal knowledge, though it has neglected some important conceptions and principles of rule of law, particularly concerning legal restrictions on arbitrary rule of government. In spite of these limitations, the program has educated millions of officials, soldiers, and ordinary citizens by giving them elementary knowledge of statutes, precedents, rules, and procedures in criminal, civil, and administrative laws. It has taught them the legal rights and obligations of citizens, and ways of protecting their interests through the law." See: Gu Su. (2003). "Progress and Problems with the Rule of Law in China," *Contemporary Chinese Thought* 34(3): 55-67. P. 62.

131 Yanrong Zhao. (2017). "The Courts' Active Role in the Striving for Judicial Independence in China," *Frontiers of Law in China* 12(2): 278-309.

132 Yanrong Zhao. (2017). "The Courts' Active Role in the Striving for Judicial Independence in China," *Frontiers of Law in China* 12(2): 278-309; Lu Xu. (2019). "The Changing Perspectives of Chinese Law: Socialist Rule of Law, Emerging Case Law and the Belt and Road Initiative," *The Chinese Journal of Global Governance* 5: 153-175.

developed systems to respond to international law and international trade issues, as a way of integrating into the global economy.[133]

However, the Constitution of China explicitly states that "[t]he People's Republic of China governs the country according to law and makes it a socialist country under rule of law[,]" and scholars have argued that the Chinese courts lack substantive authority to challenge government institutions, which are elevated above the courts. While courts are incredibly active and can apply judgements on institutions of equal or lower standing, they largely cannot judge military, intelligence, security, and political party institutions unless those institutions authorize the process of judgement.[134] As Li has written, "the courts are, on the one hand, powerful enough to be capable of corrupt conduct when dealing with groups of little or no political power and, on the other hand, entirely powerless when dealing with groups of significant political power."[135] Not all state institutions, in actuality, are similarly under the rule of law as understood in Western political systems.[136]Specifically, how China has developed and reformed its judiciary has led to concerns by Western commentators that China does not possess rule of law but, instead, rule by law. Western legal traditions understand rule of law as applying law equally to all elements of a nation-state; the executive branch is as subject to the rule of law as any other segment of society. In the case of China, the executive branch—the Chinese Communist Party and its high-level officials—are routinely identified as operating above the formal judicial system. However, due to fundamental translation challenges, assertions that China does not have rule of law, but rule by law, are often seen as being incomprehensible when translated from English. The effect is that Western critiques can be read as (when translated): 'China lacks rule of law; it, instead, has rule of law'.

---

133 Lu Xu. (2019). "The Changing Perspectives of Chinese Law: Socialist Rule of Law, Emerging Case Law and the Belt and Road Initiative," *The Chinese Journal of Global Governance* 5: 153-175.

134 Young Nam Cho. (2016). "China's "Rule of Law" Policy and Communist Party Reform," *Asian Perspective* 40: 675-697.

135 Ling Li. (2015). "Chinese Characteristics of the "Socialist Rule of Law": Will the Fourth Plenum Cure the Problems of the Chinese Legal System?" *Asian Policy* 20(July): 17-22. P. 20. See also: Ling Li. (2016). "The Chinese Communist Party and People's Courts: Judicial Dependence in China," *The American Journal of Comparative Law* 64(1): 37-74.

136 As discussed by Zhao, "the courts' refusal to take certain types of cases can be easily attributed to the weak status of the courts in China's political structure. If the superior political powers such as the CPC and the government do not wish the courts to participate in some kinds of dispute resolution process, such as the handling of politically sensitive cases, "the courts have little room to disobey."" See: Yanrong Zhao. (2017). "The Courts' Active Role in the Striving for Judicial Independence in China," Frontiers of Law in China 12(2): 278-309. 290-291.

For more, see: Lu Xu. (2019). "The Changing Perspectives of Chinese Law: Socialist Rule of Law, Emerging Case Law and the Belt and Road Initiative," *The Chinese Journal of Global Governance* 5: 153-175. See also: World Justice Project. (2019). "The World Justice Project Rule of Law Index 2019," *The World Justice Project.* Available at: https://worldjusticeproject.org/sites/default/files/documents/WJP-ROLI-2019-Single%20Page%20View-Reduced_0.pdf.

Beyond strong fundamental differences in how law operates, the Chinese judiciary is also subject to gags that can prevent a comprehensive understanding of how and why certain decisions are reached. Though the Chinese government has pushed the judiciary to publish court proceedings online—and such postings take place millions of times a year—there are carve-outs for national security cases; in these instances, the court may be prohibited from publishing a case number, date of judgement, or reasons for the judgement.[137] In fact, many judges will not even take national security cases on grounds that, "these cases were really out of the courts' ability to address. In consideration of protecting national security and maintaining social and political stability, courts also [have] refused to accept cases with political agendas."[138]

There are a number of potential implications of the Chinese legal system as it pertains to purchasing networking equipment from Huawei. To begin, any legal attempt undertaken by Huawei to prevent the Chinese government from compelling the insertion or maintenance of vulnerabilities in Huawei equipment and that butt against the Chinese government's military, intelligence, or security interests are unlikely to proceed without the approval of the Party, which has recently sought to assert comprehensive Party leadership over all elements of the government inclusive of the judiciary.[139] While Huawei has asserted that it would oppose any efforts by the Party or government to compel it to insert vulnerabilities in its equipment,[140] for such opposition to succeed, the Party or security agencies would need to lend their weight to the company's legal efforts. While not impossible, this situation suggests that efforts to rely on the Chinese judicial system will, in principle, come down to a question of politics: would the litigant—Huawei— have sufficient political clout to ultimately empower the judiciary to hear, let alone fairly decide, the case? And, if so, would any decision that turned against a litigant, such as Huawei, be published, or would it remain unpublished to the detriment of third-parties seeking to understand whether the Chinese government had issued an order that compelled Huawei to facilitate the government's surveillance efforts?

Canadians have good reason to be dubious of the genuine independence of Chinese courts when it comes to Huawei. When the Canadian government arrested Huawei's Chief

137 Lu Xu. (2019). "The Changing Perspectives of Chinese Law: Socialist Rule of Law, Emerging Case Law and the Belt and Road Initiative," *The Chinese Journal of Global Governance* 5: 153-175.

138 Yanrong Zhao. (2017). "The Courts' Active Role in the Striving for Judicial Independence in China," Frontiers of Law in China 12(2): 278-309. P. 291.

139 Jamie P. Horsley. (2019). "Party Leadership and Rule of Law in the Xi Jinping Era," *The Brookings Institute*. Available at: https://www.brookings.edu/wp-content/uploads/2019/09/FP_20190930_china_legal_development_horsley.pdf.

140 CBS News. (2019). "Huawei founder says he would defy Chinese law on intelligence gathering," *CBS*. Available at: https://www.cbsnews.com/news/huawei-president-ren-zhengfei-says-he-would-defy-chinese-law-on-intelligence-gathering/.

Financial Officer, Meng Wanzhou, in response to a US extradition request, Chinese courts quickly reassessed previously decided cases to sentence Canadians to death,[141] and seized two other Canadians who have been held without access to counsel for extended periods of time in conditions that would amount to torture in the Canadian criminal justice system.[142] In doing so, the Chinese government laid bare how politicized their court systems could become when nations take positions that run counter to perceived Chinese interests. There is little hope that a Chinese judiciary can independently adjudicate such cases or appeals without the support of the Chinese Communist Party. This speaks to the potential for Canadians to be detrimentally affected by the Chinese government should the Canadian government act now or in the future in ways that are perceived as detrimental to the Chinese government's interests.

China, like other nations, identifies a vast swathe of areas as falling under the auspices of national security,[143] arguably up to and including activities that are designed to steal intellectual property to advance Chinese five-year plans and develop critical sectors of the economy to enable Chinese sovereignty. Given that many of the concerns that are raised around the potential subversion or use of Huawei equipment or business practices turn on issues linked to China's national security interests, any efforts by Canada, Canadian companies, or Huawei itself to appeal to the Chinese courts are likely to functionally amount to political exercises that may be performatively cast through the lens of law.

7.2 - Mitigations

Setting aside the complexities of the Chinese courts, it remains unclear how the Canadian government or Canadian companies can competently rely on Chinese courts to migrate any surveillance or security issues that are linked to China's military, intelligence, or security agencies' potential efforts to insert or maintain vulnerabilities in Huawei equipment. Egregious activities might be brought against Huawei Canada in Canadian courts should employees be involved in espionage or other illegal behaviours. Similar actions

141 Alexandra Ma. (2019). "China just took another step toward putting a Canadian to death, in apparent retaliation for its arrest of Huawei's CFO," *Business Insider* (May 9, 2019). Available at: https://www.businessinsider.com/china-confirms-canadian-death-sentence-apparent-retaliation-huawei-cfo-2019-5.

142 Robert Fife, Steven Chase, and Nathan VanderKlippe. (2020). "Two Canadians jailed in China mark 500 days in confinement," *Globe and Mail* (April 23, 2020). Available at: https://www.theglobeandmail.com/politics/article-two-canadians-jailed-in-china-mark-500-days-in-confinement/.

143 Young Nam Cho. (2016). "China's "Rule of Law" Policy and Communist Party Reform," *Asian Perspective* 40: 675-697. P. 692. "The revision of the National Security Law by the Standing Committee of the National People's Congress in July 2015 and subsequent unprecedented large-scale detentions of rights lawyers and social activists demonstrate how the rule of law policy actually works in China. The national security measures defined by this law are extensive, covering eleven areas in total, including economy, society, information technology, and space as well as government, sovereignty, and national unity."

might be brought, in Canada, against suspected agents of the Chinese government who are located in Canada or operating abroad. Given that activities pertaining to the Chinese military, intelligence, and security agencies are political issues, Canada might most benefit from working with a set of other nation-states to protest or punish any actions that the Chinese government takes to the detriment of Canadian interests. The efficacy of any such measures, however, may be dubious if the failure to reverse egregious behaviour toward Canadians in Chinese prisons is any indication.

Information Box 7: The Fallibility of Canadian Bellicosity

While engaging in behaviours that parallel the bellicosity of the Chinese government may be appealing—such as suspending certain trade unilaterally and without good cause or otherwise creating a non-strategic diplomatic event—they are unlikely to promote the international order that is conducive to Canadian trading and security interests and, given the trade imbalance, are likely to be particularly damaging to Canada. Adding additional chaos to an increasingly chaotic world order is unlikely to broadly improve Canada's situation in the world, and without effective, coordinated activity with our allies or friendly middle-powers, it is unlikely that Canadian bellicosity would compel behavioural change in China.

Ultimately, then, any mitigation strategies may depend on leaning on either international organizations that China has acceded to, such as the WTO or other international fora, on the basis that China relies on international rule of law in its efforts to expand trade and diplomatic missions with foreign countries. Strategies could also involve pressuring the Chinese government to adhere to a robust domestic rule of law to demonstrate that international companies doing business with Chinese companies can be assured of the trustworthiness of Chinese companies' activities and products. Or, in perhaps a worst-case scenario, mitigation strategies might entail simply preparing for situations where the Chinese leadership could compel Huawei to secretly undertake activities. Strong and positive relations with the company, itself, may be leveraged to reveal whether it has quietly initiated legal action against the state should China compel the company to undertake activities contrary to the interests of Canadian telecommunications companies or the Canadian government. But again, the capability of such relationships to bear fruit is unclear. Should the government become aware of any such challenge, however, it might use that information on the international stage to compel fairer judicial decisions, though without guarantee that such a decision would be reached. In the long run, any judicial intervention in China that is linked with military, intelligence, or security interests and Huawei is likely to turn on political force and influence, as opposed to well-crafted or erudite legal argumentation.

8. Canada's Huawei Balancing Act

The question of whether to allow, ban, or partially ban Huawei 5G equipment has become a particularly complicated policy issue for the Canadian government, given pressures from the United States, from China, and from Canada's allies in the Five Eyes intelligence alliance. The decision matrix concerning whether Canadian telecommunications may utilize Huawei 5G networking appliances has changed as the winds of politics have shifted—domestically and internationally—and as anti-China sentiment has risen alongside American trade sanctions that now threaten Huawei's ability to produce and deliver next-general appliances.

In more detail, as of writing, the Canadian government has transitioned from being commanded by a majority-party to a minority parliament, which forces the ruling Liberal Party to assess whether its decisions concerning Huawei may be overturned by a combined set of opposition parties, with the official opposition having strong asserted that it does not believe that Huawei equipment should be permitted in Canada's next-generation (or, even, current generation) networking infrastructures[144] and passing a non-binding resolution compelling the Government of Canada to issue a decision regarding Huawei by December 2020 or January 2021.[145] A conflict between the Canadian Security Intelligence Service (CSIS) and Communications Security Establishment (CSE) about the threats posed by next-generation Huawei equipment has further sapped the government's ability to clearly assert that the equipment does, or does not, pose a threat and thus merits approval, partial approval, or a ban from Canadian networks.[146] Further, there is rising anti-Chinese sentiment in the country and, given the status of the minority government, any decisions concerning Huawei will likely be made at least in part with regard to the political implications of approving or banning the vendor.

At the same time, foreign affairs issues plague the Huawei file. To the south, the United States—Canada's largest trading partner and principal security ally—has called on Canada to ban Huawei on national security grounds while simultaneously threatening that not

---

144 Conservative Party of Canada. (2020). "Trudeau still refuses to block Huawei," *Conservative Party of Canada.* Available at: https://www.conservative.ca/cpc/trudeau-still-refuses-to-ban-huawei/; Jim Bronskill. (2020). "Political parties at odds as Ottawa nears 5G decision on Huawei," *The Canadian Press*. Available at: https://nationalpost.com/news/political-pressure-mounts-as-ottawa-moves-closer-to-5g-decision-on-huawei; Nathan VanderKlippe. (2020). "In selecting Erin O'Toole, Conservatives elevate hawkish voice on China," *Globe and Mail.* Available at: https://www.theglobeandmail.com/world/article-in-selecting-erin-otoole-conservatives-elevate-hawkish-voice-on/.

145 Steven Chase. (2020). "Opposition defeats Liberals on motion to fight Chinese tactics," *The Globe and Mail.* Available at: https://www.theglobeandmail.com/politics/article-mps-vote-to-urge-action-on-chinese-state-interference-and-huawei-5g/.

146 Steven Chase. (2019). "Canadian intelligence agencies at odds over whether to ban Huawei from 5G networks: official," *Globe and Mail.* Available at: https://www.theglobeandmail.com/politics/article-canadian-intelligence-agencies-disagree-on-whether-to-ban-huawei-from/.

acquiescing to American demands will lead to a cessation of the historical intelligence sharing and coordination that occurs between Canadian and American intelligence and security agencies.[147] Moreover, as Canadian authorities have detained Huawei's Chief Financial Officer—who is also the daughter of the company's founder—as a result of an extradition process initiated by the United States government, the United States has not substantively stood up for Canada as the country has faced reprisals from China in response to proceeding through the extradition process. And, finally, the United States has become particularly hostile when it comes to trading issues and has identified Canadian exports as posing national security threats to the United States.[148] In aggregate, Canada's southern neighbour has thrown into question the genuine strength of the friendship and alliance that Canada has historically relied on for stabilizing its international affairs.

Simultaneously, China has placed pressures on the Canadian government. Following the arrest of the Huawei CFO—and subsequent release on bail to freely move around Vancouver and live in her two mansions—China seized a pair of Canadian citizens and has subjected them to inhumane conditions that have been criticized as equivalent to torture[149] and resentenced other Canadians in Chinese prisons to death.[150] Canada is also attempting to expand its trading relationships throughout Asia and, as such, must be mindful of the regional pressures that China may bring to bear to advance or inhibit these efforts in its regional sphere of influence. Beyond the politics at play, the Chinese government has also passed security legislation that Western analysts believe authorizes the Chinese government to compel Chinese companies or their employees to repurpose telecommunications equipment for state surveillance, to the potential detriment of Canadian economic and national security interests.[151] Finally, the Chinese govern-

147 Katie Simpson. (2020). "State Department says U.S. will reassess intelligence-sharing with Canada if it lets Huawei into 5G," *CBC.* Available at: https://www.cbc.ca/news/politics/huawei-5g-state-department-trudeau-china-1.5598548. It is worth recognizing that in lower-level discussions, American officials have indicated that a full cessation of the intelligence-sharing relationship is unlikely. For more, see: CDA Institute. (2020). "All Eyes on 5G," CDAI Webinar. Available at: https://cdainstitute.ca/all-five-eyes-on-5g/.

148 Jordan Press. (2018). "Lighthizer calls Canada a national security threat in defence of steel tariffs," *Globe and Mail.* Available at: https://www.theglobeandmail.com/business/article-lighthizer-calls-canada-a-national-security-threat-in-defence-of-steel/.

149 Nathan VanderKlippe. (2019). "Two Canadians detained in China for four months prevented from going outside, official says," *Globe and Mail.* Available at: https://www.theglobeandmail.com/world/article-two-canadians-detained-in-china-are-prevented-from-seeing-the-sun-or/.

150 Associated Press. (2020). "China sentences 4th Canadian to death on drug charges in 2 years," *CBC*. Available at: https://www.cbc.ca/news/world/canadian-death-sentence-china-1.5677675.

151 Specific concerns have been raised by critical commentators about the National Intelligence Law, Counterespionage Law, and the Cybersecurity Law. See: Murray Scot Tanner. (2017). "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*. Available at: https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; Jason Silver. (2015). "China's Asymmetric Intelligence Advantage: The State Security Law," Orbis 59(3); Valentin Weber. (2019). "Finding a European response to Huawei's 5G ambitions," *Norwegian Institute of International Affairs*. Available at: https://pdfs.semanticscholar.org/d308/3c6dbb9c7b9234f836e27ee11713da3317e9.pdf.

ment has indicated that it will not be held to historical agreements that might restrict its autocratic behaviour, as demonstrated in its efforts to impose more direct Chinese rule upon Hong Kong and passage of the aforementioned security legislation.

Information Box 8: A Need for Integrated Strategies

Balancing the Huawei problem will almost certainly involve a degree of risk and cost. But in addressing the problem as a Huawei problem, the Government of Canada runs the risk of missing the forest for the trees: Canada does not need a Huawei policy per se but, instead, needs a principle-driven set of integrated industrial, cybersecurity, and foreign policy strategies. These strategies must be operationalized at the policy level so as to mitigate (in this case) the risks linked with all vendors' 5G networking appliances, and they must broadly seek to address risks, threats, and opportunities facing Canada as it moves to further digitize its economy.

While the Government of Canada is trying to thread a needle between conflicting American and Chinese interests, the decisions of some of its closest allies have increasingly boxed Canada in concerning how it can establish its own Huawei policy. While the British had initially chosen to partially ban Huawei 5G equipment, the government has since reversed that decision as a result of US trade sanctions against Huawei. These sanctions risk decreasing the security properties of Huawei's networking appliances and associated systems, which suggests that merely reviewing Huawei equipment cannot adequately mitigate the security risks linked with the company's products. The Australians have chosen to ban Huawei outright, and the Government of New Zealand has adopted security-based assessments of all vendors' products which have—to date—only blocked substantial Huawei investments in the country's networks.

In short, the Canadian government cannot point to its closest intelligence allies to find a solution that is anything other than a functional ban of Huawei equipment, nor can it make a similar decision for fear of how it will affect hostages that China is holding or Canadians' broader economic interests in Asia and foreign investment opportunities for Canadian businesses. And finally, due to how widely Canadian telecommunications companies have adopted Huawei equipment into their 4G networks, the practical costs of a Huawei ban may prevent the government from retroactively banning Huawei's products. Going forward, the Canadian government needs to develop an actionable strategic approach to address the wide breadth of issues that Huawei brings to light.

For an opposing view, see: Chen Jihon and Jianwei Fang. (2018). "Before the Federal Communications commission," *FCC*. Available at: https://thechinacollection.org/wp-content/uploads/2019/03/Huawei-Declaration.pdf.

8.1 - Elements of a 5G Strategy

The Government of Canada will need to balance its 5G Strategy alongside its broader government strategies, but there are some essential elements that should be included in whatever the government ultimately produces. In what follows, I briefly outline a set of policies that could be included as part of a broader strategy designed to enhance the resiliency, security, and availability of 5G technologies. Each policy is selected from the Mitigation sections that appeared earlier in this report. However, rather than any particular element being adopted, the policies should follow from an actionable and holistic strategy that involves an all-of-government effort and that is designed so that Canadians, businesses, allies, and competitors can all appreciate the rationale behind the strategy and can predict future government policy decisions.

8.1.1 - Protecting and Developing Intellectual Property Expertise

Huawei has, and continues to, prolifically invest in developing intellectual property, and the company actively shapes standards through international standards bodies. To strengthen Huawei's competitors—to ensure that no single vendor achieves massive market dominance—the Government of Canada could explore or adopt policies to diversify the players who develop networking standards and patents, and it could focus attention on projects designed to reduce vendor lock-in writ large.

The Government of Canada has previously provided funding to Huawei's competitors in an effort to enhance those companies' research and development capacity. In the absence of North American competitor companies, such as Nortel or Cisco, the government could continue to provide some funding to competitor companies to avoid the risk that Ericsson or Nokia are less able to produce high-quality 5G and (in the future) 6G networking appliances. Companies might be required to set up R&D facilitates in Canada to better retain Canadian expertise.

By providing increased funding to Canadian universities to foster basic research that is not vested with foreign companies, the government might address concerns that are linked to Canadian researchers becoming dependent on foreign funding. Canadian academics are well regarded internationally for their expertise in next-generation technologies, including those pertaining to next-generation communications systems. Any government actions designed to merely discourage or bar academics from seeking foreign companies' funding, however, would risk either decreasing universities' research productivity or encouraging academics to leave for institutions that were capable of providing the resources that they need to conduct their research. Alternately, should the Canadian

government not want to discourage Canadian academics from seeking funding from foreign companies or increase basic research funding to universities, the government should provide public briefing materials so that universities can craft responsible policies in light of perceived difficulties linked to foreign funding

The Government of Canada could also provide funding for academic and non-academic researchers or organizations to contribute to the OpenRAN Project. This project is focused on creating radio access networks that are based on vendor-neutral hardware and software. OpenRAN is focused, in part, on reducing vendor lock-in by enabling telecommunication carriers to minimize the amount of proprietary hardware in their networks and facilitating the purchase of off-the-shelf hardware.

Finally, the Government of Canada can and should develop mechanisms to encourage private individuals, businesses, or non-profit organizations to participate in networking standards setting. Tax benefits could be assigned where Canadian persons or organizations are involved in developing these standards Such benefits can be justified on the basis that whoever helps to establish the standards will have an early appreciation for their implementation and that, in turn, could help to enable Canadian businesses to more rapidly take advantage of next-generation communications technologies. In the case of Canadian non-profit organizations and charities, the government could facilitate their inclusion by providing registration fees, travel costs, and other expenses either directly from government departments or through vehicles such as the International Development Research Centre. In addition to telecommunications standards, the government should prioritize encouraging individuals and organizations alike to take leadership roles in adjacent standards- and norms-setting processes, such as those that pertain to promulgating the availability of strong encryption and the integrity of telecommunications systems and critical infrastructure.

All of these efforts are focused principally on ensuring the availability of 5G and next-generation networking appliances and associated products. By ensuring that there is a competitive landscape of vendors, the Government of Canada can be better assured that domestic companies will not be overly beholden to a single vendor and, through that vendor, subject to undue foreign political interference in their business operations.

8.1.2 - Fostering a More Diverse Market

At present writing, there are three principal companies—Huawei, Ericsson, and Nokia—that sell a full range of 5G appliances that telecommunications providers will need to provide 5G networks to customers. Huawei's growth—and increasing dominance—in markets around the world carries with it risks of long-term vendor lock-in, the potential that their competitors will be less able to provide advanced next-generation equipment at reasonable or fair costs, and the possibility that the Chinese government could restrict

the future sale of Huawei equipment should countries adopt anti-Chinese policies.

Mitigating many of the aforementioned risks is possible by deliberately fostering a diverse telecommunications market. This could, in part, be accomplished by mandating that Canadian telecommunications companies have a certain diversity of vendors in their networks to reduce the risks linked with total vendor lock-in. Diversity may also carry security benefits, insofar as a vulnerability in a given vendor's systems would be less likely to endanger the security of a telecommunications company's entire network. Such diversification strategies also have the benefit of providing business to currently struggling companies, such as Ericsson and Nokia, and of reducing the likelihood that only one or two vendors will exist that carriers can purchase equipment from in the future. Diversification may also mean that any future efforts by the Chinese government to functionally weaponize the availability of Huawei products—similar to how the American government has used its influence over semiconductor companies to wreak havoc with Chinese companies, including Huawei—has a reduced impact on Canadian telecommunications businesses. Additionally, diversification efforts may see the Government of Canada deliberately encouraging companies to adopt OpenRAN for 5G networking appliances when that project begins to bear fruit.

In aggregate, these efforts would have the effect of enhancing the resiliency, security, and availability of 5G networking equipment. By compelling telecommunications companies to adopt a range of vendors' products in their networks, it may be more possible to remove certain companies' appliances if a specific company has been compelled to insert or retain a vulnerability in its equipment, or if access to the company's next-generation products is used as a weapon in country-to-country negotiations. Furthermore, there are security benefits linked to diversification. Namely, having a more diverse selection of vendors in Canadian telecommunications networks may reduce the risk of security class breaks, or vulnerabilities that affect the entirety of a telecommunication company's networks. Finally, by diversifying the vendors whose products are in Canadian networks, the Government of Canada would be working indirectly to ensure that Huawei's stressed competitors would be more likely to survive as they obtained Canadian companies' business.

8.1.3 - Diversified Security Processes

All telecommunications vendors' products may, and likely do, possess vulnerabilities that can sometimes be exploited, forcing the equipment to behave in a way that is contrary to the desires of either a telecommunications provider or its customers. Western nations are presently most concerned about the potential for Huawei 5G networking appliances to be exploited for espionage or disruption or attack operations, but governments around the world are presently discovering and taking advantage of vulnerabilities in existing

telecommunications appliances to undertake such operations. There is no reason to expect that, should Canadian telecommunications companies be banned from using Huawei products, that such operations will stop being effective when directed toward Canadian networks and systems.

Given that all elements of society are increasingly being integrated into digital systems that are commonly linked to the Internet, the Government of Canada should adopt processes intended to both reduce the likelihood of accidentally generated and intentionally inserted vulnerabilities being present in 5G networking appliances. And, moreover, activities should be undertaken to mitigate the likelihood that any such vulnerabilities are exploited.

First and foremost, the Government of Canada should focus on defensive information assurance. Working with close allies, this focus may involve increasing investments in the Common Criteria program or, alternately, developing review organizations paralleling the UK's HCSEC to assess non-Huawei networking appliances. Canada might focus on Ericsson, and New Zealand and Australia on Nokia and Samsung as examples. The fruits of such assessments might be shared confidentially as top-secret outputs and with the public in declassified outputs. These public outputs are particularly important to generate trust in the assessments, and they are particularly important in light of the reputational damage done following the revelations of Edward Snowden. Including additional close allies may increase the resources that can commonly be brought to bear to assess and remediate vulnerabilities that are present in hardware, firmware, or software associated with vendors' equipment. While it is almost impossible to find all vulnerabilities, by focusing attention on finding and publicly disclosing them,[152] any efforts to secretly inject or retain vulnerabilities in equipment will be that much more difficult.

Second, serious effort must be made to ensure compliance with the law when assessing product security. Canada's security intelligence and foreign signals intelligence agencies have received a range of new powers that can be applied to assessing the security of products used in critical infrastructure. Review bodies should carefully monitor the exercise of these powers to ensure that their exercise is lawful, necessary, and proportionate; it is particularly important for these bodies to ensure that the Canadian Security Intelligence Service, in particular, behaves in conformity with law. Both Canada's National

152 Though beyond the scope of this report, the Government of Canada should also adopt a robust vulnerabilities equities program to ensure that found vulnerabilities are actually disclosed instead of retained for government security or intelligence operations. For more, see: Christopher Parsons. (2019). "Cybersecurity in the Financial Sector as a National Economic Security Issue," Standing Committee on Public Safety and National Security, February 2019.

Security and Intelligence Committee of Parliamentarians (NSICOP) and National Security Intelligence Review Agency (NSIRA) should pay particularly close attention to how the CSIS, CSE, and RCMP act to protect critical infrastructure, and any actions that are taken to disrupt operators who behave contrary to Canada's national interests. Such reviews will help ensure legal compliance by Canadian intelligence, security, and policing agencies and, as such, assure the public that these agencies can be trusted to protect Canadian interests without behaving illicitly.

Third, the Government of Canada should actively work to ensure that private companies can identify threats to their networks and customers in the most effective and secure way possible. Private companies will continue to be the principal parties who are responsible for defending Canada's telecommunications landscape, and actions that undermine or get in the way of such activities should be avoided. This means, in part, working with industry to assist in how threat indicators are shared between industry and government, as well as investing in research to investigate how machine learning can be used to enhance network defences. Working with private companies may also mean tasking the CRTC with the responsibility of assessing and confirming that Canadian telecommunications companies are enabling all of the security elements associated with the 5G standards to provide baseline levels of security on Canadian networks. Finally, government policies that threaten the ability to secure data—such as threats by the Canadian government to remove the availability of end-to-end encryption—should be set aside in favour of policies that would enhance the availability of strong encryption. In aggregate, a defence-first approach must be taken to secure critical infrastructure; infrastructures' security properties should not be deliberately weakened on the prayer that adversaries will not take advantage of what will otherwise almost certainly become well-known and publicized security deficiencies.

The aforementioned policies are designed, first and foremost, to ensure that networks that all Canadians rely on are secure. None, of course, entirely eliminate risks. But, if well-coordinated and applied, such policies would increase the friction that adversaries would need to overcome to conduct espionage, disruption, or attack operations through Canadian telecommunications networks. Similarly, the aforementioned policies would broadly increase the resilience of Canadian telecommunications networks. In addition to increasing the security properties associated with Canada's 5G infrastructures, developing robust and resilient policies to accompany technical defences will serve to improve government's ability to coordinate responses in the face of adversarial actions taken toward Canadian critical infrastructure while enhancing the government's abilities to project its—and Canadians'—interests to the rest of the world. Importantly, these policies should be implemented *regardless* of whether Huawei is permitted, partially banned, or fully banned from Canadian telecommunications networks. All vendors' products can

contain vulnerabilities, and it is in Canadians' best interest to reduce the threats that vulnerabilities pose regardless of where the vendor happens to be headquartered.

9. Conclusion

5G encompasses a set of networking technologies that will be deployed throughout Canada over the coming years. Canadian companies are beginning to deploy 5G networks and mobile phone providers are selling 5G-compatible devices. Unlike in past networking evolutions, the most prominent and competitive vendor currently selling 5G equipment to telecommunications providers is a Chinese company, Huawei. As a result, worries about potential Chinese espionage, disruption, and attack capabilities that could be conducted using potentially privileged information about Huawei products have been heightened. Moreover, and in excess of theoretical concerns about Chinese operations, China's leadership has routinely shown that they may punish foreign countries and their industries in order to encourage China-friendly policies and decisions. Simultaneously, the Chinese Communist Party Committees in state, semi-state, and private businesses have increased their influence over how companies operate internally and externally. In aggregate, the concerns associated with Huawei 5G networking equipment are significantly linked to concerns about how China might behave, geopolitically, into the future.

It is in this context that the Government of Canada is attempting to craft a policy concerning the conditions upon which 5G equipment vendors will be permitted to sell 5G equipment to Canadian telecommunications companies. To some extent, the Government of Canada's decision to avoid making a decision about banning or restricting the use of Huawei 5G equipment has been entirely rational. Indeed, while some have worried that Canada is behind the curve in making a decision about whether to ban Huawei products, the government can now make decisions based on lessons learned from its closest allies. However, it is becoming increasingly important for the government to adopt a clear security posture with regard to the products and vendors it will allow into Canadian networks, given that Canadian companies are in the process of investing billions of dollars in 5G infrastructure.

As this report showcases, there are numerous equities that must be balanced when determining what, if any, roles Huawei equipment should play in Canada's 5G networks. With only the benefit of open-source information, it is clear that while 5G technologies could enable new lines of innovation, the technologies are also accompanied by a range of risks. These risks are not all equivalent, nor will they necessarily all come to light. Some may be easier to mitigate than others. And some risks, such as those linked with technical vulnerabilities, are not solely restricted to 5G products sold by Chinese companies such as Huawei. Monitoring for whether and, if so, how Chinese operators (and those operating at the behest of other states) are exploiting products sold by Huawei and its competitors

will be critical to better secure Canadian interests. Evaluating all companies' 5G equipment for security deficits should be adopted as a best, and necessary, practice.

A mix of mitigations will be needed to reduce the risks that the government, private companies, and external stakeholders believe are more probable or most problematic. No mitigation strategy will ever be perfect. Making a decision to ban Huawei from selling 5G equipment to Canadian telecommunications providers, as an example, will not solve the issue of foreign operators conducting espionage, disruption, or attack operations against the Government of Canada, private companies, or private persons who rely on non-Huawei equipment. Nor would a ban clearly address intellectual property or trading concerns linked with Huawei and China more broadly. Rather than trying to solve a Huawei problem, the Government of Canada should develop an integrated set of industrial, cybersecurity, and foreign policy strategies that are operationalized so as to mitigate the risks linked with all vendors' 5G networking appliances and that broadly seeks to address risks, threats, and opportunities that face Canada as it moves to further digitize its economy.

This report has not specifically recommended product choices, nor explicitly called for banning Huawei or any other company from specific parts of Canadian telecommunications or critical industry networks. These decisions need to be made in consultation with network operators, government agencies, and other parties with expert knowledge concerning intellectual property, trade, technical security, and national security. It is my hope that this report, in its entirety, has laid bare why this interwoven set of experts and groups is necessary and why any effort to address issues linked with Huawei products in isolation will almost certainly fail to functionally address the broad constellation of political, technological, and security issues that are intrinsically linked to 5G technologies.